Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Huawei Designation	)	PS Docket No. 19-351

COMMENTS OF HUAWEI TECHNOLOGIES CO., LTD., AND HUAWEI TECHNOLOGIES USA, INC.

Glen D. Nager
Michael A. Carvin
Shay Dvoretzky

JONES DAY
51 Louisiana Ave., NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
macarvin@jonesday.com
sdvoretzky@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

Counsel to Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc.

February 3, 2020

SUMMARY

The Bureau must reject the Commission's initial designation of Huawei and decline to enter a final designation against Huawei. As the Report and Order makes clear, the designation was not based on a sober, objective assessment of reliable evidence developed and considered through a fair and lawful process, but rather a gerrymandered recitation of *ad hoc*, Huawei-specific conclusions designed to implement a campaign by certain government officials, including members of Congress, to single out Huawei for burdensome and stigmatizing restrictions; put it out of business in the United States; and impugn its reputation around the world. Unsurprisingly, this effort was unlawful and misguided. In issuing the initial designation and the underlying rule upon which it was based, the Commission exceeded its statutory authority; failed to give Huawei notice that it was being subjected to an adjudication or notice of the standards under which it is being judged; failed to treat similarly situated entities in a like manner; and relied on half-truths and unsupported claims about Huawei to support its conclusions.

Now the Commission's initial designation is before the Bureau, which the Commission evidently expects to rubber stamp its determination. But the Bureau should not further this infirm and legally unsupported process by converting the Commission's existing designation into a final designation under the rule, for at least three fundamental reasons.

First, the Commission's initial designation cannot support a final designation of Huawei. Even leaving aside the numerous legal infirmities identified to the Commission during its putative rulemaking, the initial designation is unsupported by a preponderance of the evidence that was before the Commission, and was based in large part on nonevidence and unreliable evidence that should not have been considered. The initial designation also relied on unsupported conclusions about Chinese law that ignored Huawei's multiple expert submissions. In addition, it arbitrarily

and capriciously treated Huawei differently from other similarly situated telecommunications companies with equal or greater ties to China, without any justification. The only explanation for this selective targeting of Huawei is that the Commission bowed to unconstitutional congressional pressure and made its decision based on irrational and unconstitutional prejudgment against Huawei.

Second, additional evidence that Huawei has submitted with these Comments further demonstrates that final designation of Huawei would be improper. Because the Commission failed to give Huawei notice of the standard to be applied against it, the facts to be assessed under that standard, or even the fact that Huawei was being adjudicated, much of this evidence responds to the apparent ad hoc considerations and unsubstantiated conclusions the Commission has relied on to designate Huawei, to the extent that these can be deduced from the Commission's designation.

Third, even leaving the foregoing problems to one side, the Bureau cannot lawfully enter a final designation of Huawei without providing Huawei with additional procedural safeguards required by statute, Commission regulation, and the Fifth Amendment's Due Process Clause. In particular, Huawei is entitled—at minimum—to notice of the supposed evidence against it and the Bureau's reasons for believing that that evidence warrants final designation; an opportunity to respond to that evidence, including the right to cross-examine any witnesses against it, especially where (as here) facts apparently material to the Commission's decision are in dispute; an impartial decisionmaker unaffected by bias, prejudice, or prejudgment; and proceedings free from ex parte contacts.

Huawei recognizes the Bureau's unenviable position. The Commission has directed the Bureau to implement a foregone judgment that neither the Commission nor the Bureau has statu-

tory (or constitutional authority) to make. Compounding the problem, the Commission has articulated no substantive legal standard for making a final designation, or any criteria for applying a standard, leaving the Bureau (and Huawei) with no objective guidance about how to apply the Commission's rule. Even so, the Commission has announced that it is "confident" that Huawei satisfies whatever the standard might be, and expects the Bureau to obligingly enter a final designation against Huawei. The Constitution and American rule of law demand better. The Bureau should resist the Commission's invitation to participate in this deeply flawed exercise, and decline to finally designate Huawei under the rule.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Huawei Designation	)	PS Docket No. 19-351

COMMENTS OF HUAWEI TECHNOLOGIES CO., LTD.,
AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd. ("Huawei Technologies") and Huawei Technologies USA, Inc. ("Huawei USA" and, together with Huawei Technologies, "Huawei"[1]), by its undersigned counsel, submit these comments in response to the Report and Order, Further Notice of Proposed Rulemaking, and Order released in WC Docket No. 18-89 and PS Docket No. 19-351 on November 26, 2019, by the Federal Communications Commission ("FCC" or "Commission") and published in the *Federal Register* on January 3, 2020, at 85 Fed. Reg. 230, and in response to the Public Notice issued by the Public Safety and Homeland Security Bureau ("Bureau") on January 3, 2020, in PS Docket No. 19-351.

INTRODUCTION

As Huawei has explained throughout the course of this proceeding, the Universal Service Fund ("USF") rule that the Commission adopted in its Report and Order ("Order") and the procedure that led to Huawei's initial designation were contrary to law and fundamentally flawed. The

[1] Because many of the arguments in these comments apply to both Huawei Technologies and Huawei USA, these comments refer to these two entities collectively as "Huawei." But the two entities are distinct, and as explained below, it was irrational and unlawful for the Commission not to conduct individualized assessments for each entity, and to instead make a blanket designation against "Huawei Technologies Company, its parents, affiliates, and subsidiaries." Order ¶ 58; *see infra* pp. 105-14. It would be equally irrational and unlawful for the Bureau to make the same mistake now.

Order makes clear that the rule and initial designation were not based on a sober, objective assessment of reliable facts and possible regulatory options; developed and considered through a fair and lawful process; or evaluated against an intelligible, generally applicable standard. Rather, the rule and designation were gerrymandered actions designed to implement a campaign by certain government officials, including members of Congress, to single out Huawei for burdensome and stigmatizing restrictions, put it out of business in the United States, and impugn its reputation here and around the world.

The Commission now evidently expects that, despite these legal infirmities, the Bureau will rubber-stamp its determination and convert the Commission's initial designation of Huawei into a final designation. But the Bureau should decline to do so, for at least three fundamental reasons.

First, the Commission's initial designation cannot form the basis for a valid final designation of Huawei. Even leaving aside the numerous legal infirmities in the initial designation and underlying rule that Huawei has already raised—all of which would necessarily infect any final designation—the initial designation is unsupported by a preponderance of the evidence that was before the Commission, and was based in large part on nonevidence and unreliable evidence that should not have been considered. The initial designation also relied on unsupported conclusions about Chinese law that ignored Huawei's multiple expert submissions; arbitrarily and capriciously treated Huawei differently from other similarly situated telecommunications companies with equal or greater ties to China; and was infected by unconstitutional congressional pressure and prejudgment against Huawei.

Second, additional evidence that Huawei has submitted in connection with these Comments further demonstrates that final designation of Huawei would be improper. Because the Commission failed to give Huawei notice of the standard to be applied against it, the facts to be assessed under that standard, or even the fact that it was being adjudicated, Huawei necessarily focused its submission of new evidence on the apparent ad hoc considerations and unsubstantiated conclusions the Commission relied upon to designate Huawei, to the extent that these can be deduced from the Commission's designation.

Third, and in any event, the Bureau cannot lawfully enter a final designation as to Huawei without providing it with additional legally required procedural safeguards. In particular, Huawei is entitled, at minimum, to notice of the evidence against it and the Bureau's reasons for believing that evidence warrants final designation; an opportunity to respond to the evidence, including the right to cross-examine any witnesses against it; an impartial decisionmaker unaffected by bias, prejudice, or prejudgment; and proceedings free of ex parte contacts.

Huawei recognizes that the Commission has placed the Bureau in an untenable position in these proceedings. It has tasked the Bureau with implementing a judgment based on a legal standard as to which the Commission has offered no guidance, at the end of an adjudicatory process about which Huawei had no prior notice, and in which Huawei has had no adequate opportunity to be heard and no meaningful procedural protections that would ensure an objective and unbiased result. And, to make matters worse, the Commission itself—the entity with final authority to review and disapprove the Bureau's decision with respect to a final designation—has made abundantly clear that it is already "confident" that Huawei presents a national security threat, based on a record that fails to support any such judgment. Order ¶ 54. The Commission's evident expectation that the Bureau will obligingly echo this preordained conclusion doubtlessly leaves the Bureau

in a difficult spot. Nonetheless, the Bureau should resist the Commission's invitation to participate in this deeply flawed exercise and decline to finally designate Huawei under the rule.

BACKGROUND

I. Huawei is a global technology company dedicated to cybersecurity

Huawei Technologies is a global leader in information and communications technology ("ICT") products and services. It was established in 1987 through private investment in Shenzhen, Guangdong Province, where it is still headquartered. Although the company initially focused on providing connectivity to rural areas of China, today Huawei's multinational operations support more than 500 major telecommunications operators across more than 170 countries. Exhibit 1-C, Declaration of Thomas Dowding ¶ 7 (submitted as Ex. C to 6/1/2018 Huawei Comments) ("6/1/2018 Dowding Decl."). To provide sustainable equipment and service to its widespread customer base, Huawei established a global supply chain, procuring components, spares, equipment, software, and service from suppliers located in the U.S., Europe, Asia, and other regions. *See* Ex. 1, 6/1/2018 Huawei Comments at 5 ("6/1/2018 Huawei Comments").

Huawei launched operations in the United States in 2001. Huawei currently has three operating entities in the United States: (1) Huawei USA; (2) Huawei Device USA Inc. ("Huawei Device USA"); and (3) Futurewei Technologies, Inc. ("Futurewei") (together the "U.S. Operating Subsidiaries"). 6/1/2018 Dowding Decl. ¶ 19. Huawei USA is the only Huawei-affiliated entity authorized to sell telecommunications infrastructure products and services to carriers in the United States. *Id.* ¶ 22. Huawei Device USA focuses on Huawei's consumer businesses, such as sale of handsets and other consumer devices, while Futurewei handles research and development in the United States. Ex. B, Declaration of Thomas Dowding ¶ 13 n.2 ("2/3/2020 Dowding Decl.").

Huawei is—and always has been—a private company. Huawei Technologies, Huawei USA, and the other two U.S. operating entities are all wholly owned direct or indirect subsidiaries

of Huawei Investment & Holding Co., Ltd. ("Huawei Holding"). Huawei Holding is a private company, owned entirely by Huawei's founder, Mr. Ren Zhengfei, and it employees, through an employee stock ownership plan in which 96,768 employees participated as of the end of 2018. 6/1/2018 Dowding Decl. ¶ 10; Ex. E, Declaration of Leon Wang ¶¶ 4-5 ("1/23/20 Wang Decl."); Ex. QQ, 2018 Huawei Annual Report ("2018 Huawei Annual Report"). No Chinese government agency or outside organization holds shares in Huawei. 2018 Huawei Annual Report at 1; 1/23/20 Wang Decl. ¶ 15.

Huawei's corporate governance structure spans a number of different groups and committees. At the highest level, corporate oversight of Huawei is carried out by a Board of Directors (the "Board"),[2] which is responsible for, among other things, reviewing and approving all plans for entering industries or strategic changes; organizational restructuring; financial policies and business transactions; internal controls and operational compliance systems; and the employment of senior management. 2018 Huawei Annual Report at 132. Chairmen take turns leading the Board and its Executive Committee. Currently, 17 private citizens comprise the Board. *Id.*; *see also* 6/1/2018 Dowding Decl. ¶ 16. Huawei's financial statements are audited by an independent third-party organization; since 2000, Huawei's auditor has been KPMG. 2018 Annual Report at 70-126 (providing auditor's statement and audited consolidated financial statements); *see also* Ex. MM, Huawei, Independent Auditor.

Huawei's products and services encompass four sectors. 6/1/2018 Dowding Decl. ¶ 8. First, Huawei supports international carriers through its Internet of Things ("IoT"), All-Cloud, and

[2] Each of the five Huawei entities described above has its own Board of Directors (or, in the case of Huawei Device USA, a single director). Wang Decl. ¶ 4. Currently, there are 17 individuals who serve as members of both the Huawei Holding and Huawei Technologies Boards of Directors (referred to as the "Board" and "Huawei Board Members").

5G offerings, among other telecommunications products and services. *Id*. Second, Huawei's enterprise business supports nearly 200 Fortune Global 500 companies through its products in cloud, big data, OpenStack software tools, data centers, and IoT. *Id*. Third, Huawei's growing consumer business offers world-class smart devices—in 2017 alone Huawei shipped 153 million smartphones worldwide. *Id.* Fourth, Huawei launched its Cloud Business Unit in 2017, which includes 99 services across 14 major categories, with applications in manufacturing, healthcare, e-commerce, and connected vehicles. *Id*.

Huawei USA brought advanced technology and much needed competition to the United States. Various studies have shown that the United States' telecommunications infrastructure is falling behind those in other developed countries. *Id*. ¶ 28. And equipment prices in the United States tend to be about 20% to 30% higher than in other developed regions because only two companies—Nokia and Ericsson—dominate the market. *Id*. ¶ 25; *see* Ex. I, Expert Report of Dr. Debra J. Aron ¶¶ 17-18 ("Aron Report II"). Huawei USA's participation in the U.S. market drives down prices, increases deployment by carriers, and strengthens telecommunications infrastructure. Ex. 1-F, Declaration of Allan L. Shampine ¶ 7, 13 (submitted as Ex. F to 6/1/2018 Huawei Comments) ("Shampine Decl."). For example, Huawei's 4T4R Single Radio Area Network ("RAN") products helped Huawei's U.S. carrier clients improve their service area coverage by 30%. 6/1/2018 Dowding Decl. ¶ 29.

Although Huawei USA's sales grew through the 2000s, those sales have declined since roughly 2012. This decline coincided with the October 8, 2012, publication by the U.S. House of Representatives Permanent Select Committee on Intelligence of its *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* ("HPSCI Report"), and the beginning of the ongoing agitation and interference by various U.S.

Government officials and agencies in private business dealings between Huawei and its customers. *See, e.g.*, 6/1/2018 Dowding Decl. ¶ 33. Despite these challenges, Huawei has never faltered in its commitment to the U.S. market. Approximately 25% of Huawei's 263 suppliers in 2017 were U.S.-based. Huawei's procurement from U.S. suppliers—totaling more than $20 billion—account for a large portion of its supply chain. 6/1/2018 Huawei Comments at 5. And, as of April 2018, Huawei USA has employed over 1,200 employees across 13 offices and six R&D centers in the U.S., including in Silicon Valley; Bridgewater, New Jersey; Chicago, Illinois; and San Diego, California. *See* 6/1/2018 Dowding Decl. ¶ 21; *see, e.g.*, Ex. NN, Zen Soo, *Huawei Is in Better Shape to Withstand US Pressure, Thanks to Industry's Largest Research Budget*, South China Morning Post (Apr. 26, 2018).

As both an important social responsibility and a key commercial interest, Huawei considers cybersecurity paramount. Huawei has established and implemented an end-to-end global cybersecurity system through stringent security policies and processes that reflect international standards and guidelines; local laws and regulations; and feedback from vendors, employees, suppliers, and customers. Ex. 1-B, Declaration of Donald Purdy, Jr. ¶¶ 10-18 (submitted as Ex. B to 6/1/2018 Huawei Comments) ("6/1/2018 Purdy Decl."). Huawei's commitment to cybersecurity extends through its corporate leadership and to all its employees under a robust internal compliance program that includes routine processes for self-checks. *Id*. ¶¶ 17, 22-23. In addition to Huawei's stringent global policies on cybersecurity and privacy, Huawei USA implements U.S.-specific policies to ensure compliance with U.S. statutes, regulations, customer requirements, and industry standards that build upon Huawei global practices. *Id*. ¶¶ 19-20. Huawei USA has a separate Cybersecurity and Privacy Committee chaired by its Chief Security Officer, with members appointed by Huawei USA executives. *Id*. ¶ 21.

II. The Commission's Order targeted Huawei and ZTE in an adjudication disguised as a rulemaking

The procedural history of these proceedings demonstrates that, from their start, they have been fundamentally flawed and motivated by transparently political prejudgment of Huawei.

A. Members of Congress write to Chairman Pai about Huawei

These proceedings have their origins in a December 20, 2017, letter that Senator Tom Cotton and 17 other members of Congress sent to Chairman Pai, expressing their "concern[] about Chinese espionage in general, and Huawei's role in that espionage in particular." 12/20/2017 Cotton Letter; *see also* Order ¶ 11. The members' "concern" was based on a 2012 Report prepared by the House Permanent Select Committee on Intelligence ("HPSCI"), which, more than eight years earlier, had purported to conduct an investigation "into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States." HPSCI Report iv. Based on this Report, these members of Congress told Chairman Pai that "Huawei … cannot be trusted to be free of foreign state influence and thus poses a security threat to the United States and to our systems." 12/20/2017 Cotton Letter.

Notably, HPSCI conceded in its Report that it had not conducted "a review of all technological vulnerabilities of particular ZTE and Huawei products or components." HPSCI Report at 11. Rather, the Committee tentatively observed that Huawei "*may* have connections and ties to Chinese leadership," *id.* at 24 (emphasis added); noted that it is "*possible* that Huawei receives substantial support from the Chinese government," *id.* at 30 (emphasis added); and expressed "serious *doubts* about whether Huawei can be trusted to operate in the United States in accordance with United States legal requirements and international codes of business conduct," *id.* at 13 (emphasis added). Despite this equivocation, the Committee concluded that, "[b]ased on available

classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems." *Id.* at 45.

B. The Commission issues its Notice of Proposed Rulemaking

In March of 2018, shortly after receiving the letter from members of Congress described above, Chairman Pai personally replied, stating that "[he] share[d] [their] concerns about the security threat that Huawei and other Chinese technology companies pose to our communications networks," and assured them that he intended to "take proactive steps to help ensure the integrity of the communications supply chain in the United States in the near future." Letter from Hon. Ajit Pai, Chairman, FCC, to Senator Tom Cotton, et al., U.S. Senate (Mar. 20, 2018), https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0323/DOC-349859A1.pdf ("3/20/2018 Pai Letter"). Less than a month later, the Commission issued a Notice of Proposed Rulemaking ("NPRM") seeking comment on a proposed rule that would prohibit the use of USF funds "to purchase or obtain any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain." *Protecting Against National Security Threat to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, 33 FCC Rcd. 4058, 4062, ¶ 13 (Apr. 17, 2018).

The NPRM did not define what it would mean to "pos[e] a national security threat" to communications networks or supply chains. Nor did it propose a standard or criteria by which to identify companies that posed such a threat. Instead, it asked commenters: "*How* should [the Commission] define the universe of companies covered by our proposed rule (i.e., a covered company)?" *Id.* at 4064, ¶ 19 (emphasis added). And it "s[ought] comment *broadly* on possible approaches to defining the universe of companies covered by [its] proposed rule." *Id.* (emphasis added).

The Commission claimed to propose three potential "approach[es]" for identifying "companies that pose a national security threat to the integrity of communications networks or the communications supply chain." *Id.* ¶¶ 19-22. But that list of possible "approach[es]" likewise failed to include a standard for identifying companies that would be covered by the rule. The first possible approach was "for the Commission to establish the criteria for identifying a covered company." *Id.* ¶ 20. But the Commission did not actually propose any criteria other than whether a company had already been prohibited from contracting with the government or participating in government programs. *Id.* And the Commission's two other approaches proposed to rely on (1) "existing statutes listing companies barred from providing certain equipment or services to federal agencies for national security," *id.* ¶ 21, and (2) "a federal agency other than the Commission to maintain a list of communications equipment or service providers that raise national security concerns," *id.* ¶ 22. Thus, none of the three "approaches," and nothing else in the NPRM, identified what the Commission meant by "pos[ing] a national security threat to the integrity of communications networks or the communications supply chain." *Id.* at 4064-66, ¶¶ 19-23. The NPRM also did not indicate that the Commission would conduct any adjudications of specific companies under whatever rule it might adopt simultaneously with adopting that rule. Nor did the NPRM propose any process for designating companies under any rule that the Commission might adopt.

The NPRM did make one thing clear, however: Despite a lack of standards or any concrete proposal for designating companies national security risks, and despite claims that it was engaging in a *rulemaking—i.e.*, promulgating a regulation of general, prospective applicability—the Commission initiated the rulemaking proceedings to target Huawei and ZTE. The NPRM specifically discussed Huawei and ZTE, identifying them (but no other telecommunications equipment companies) as putative threats to the security of U.S. telecommunications networks, and referenced the

HPSCI Report and provisions of the National Defense Authorization Act for Fiscal Year 2018 ("2018 NDAA") that prohibited the Department of Defense from using Huawei equipment and services in "certain critical programs, including ballistic missile defense and nuclear command, control, and communications." *Id*. at 4059-60, ¶¶ 4-6; Pub. L. No. 115-91, § 1656, 131 Stat. 1283 (Dec. 12, 2017) (prohibiting the Defense Department from procuring "covered telecommunications equipment or services," defined, in part, as "equipment produced by Huawei Technologies Company").

C. Huawei submits comments and other materials to the Commission

1. On June 1, 2018, Huawei submitted comments in response to the NPRM, in which it argued that the proposed rule prohibiting USF recipients from purchasing equipment or services from blacklisted entities suffered from multiple defects. 6/1/2018 Huawei Comments. Huawei included a substantial amount of evidence in support of its comments, including declarations and expert reports from (1) Donald A. Purdy, Jr., Chief Security Officer of Huawei USA since 2012 (6/1/2018 Purdy Decl.); (2) John Suffolk, who has forty years of experience in information communications technology and has served as Global Cyber Security and Privacy Officer for Huawei Technologies since 2011 (Ex. 1-A, Declaration of John Suffolk (submitted as Ex. A to 6/1/2018 Huawei Comments) ("Suffolk Decl.")); (3) Thomas Dowding, Senior Vice President of Sales of the Wireless Business and Smart PV Plant Solution Division for Huawei USA since 2010 (6/1/2018 Dowding Decl.); (4) Dr. Allan L. Shampine, an expert in applied microeconomic analysis (Shampine Decl.); (5) Ariel Lu Ye, who serves as a senior partner with King & Wood Mallesons in Shenzhen and is an expert in Chinese law (Ex. 1-D, Declaration of Ariel Ye (submitted as Ex. D to 6/1/2018 Huawei Comments) ("Ye Decl.")); (6) Bryant Tow, an expert in risk management and security solutions with over twenty-five years of experience managing large global cyber and physical security teams (Ex. 1-G, Declaration of Bryant Tow (submitted as Ex. G to

6/1/2018 Huawei Comments) ("Tow Decl.")); (7) Professor Emily Hammond, an expert in the field of administrative law and the Glen Earl Weston Research Professor of Law at the George Washington University Law School (Ex. 1-H, Declaration of Emily Hammond (submitted as Ex. H to 6/1/2018 Huawei Comments) ("Hammond Decl.")); (8) Jihong Chen and Jianwei Fang, experts in Chinese law who currently serve as partners at the Zhong Lun Law Firm in Beijing (Ex. 1-E, Declaration of Jihong Chen and Jiangwei Fang (submitted as Ex. E to 6/1/2018 Huawei Comments) ("Chen & Fang Decl.")).

In its NPRM comments, Huawei made four principal arguments. *First*, Huawei explained that the Commission lacked the statutory authority to prohibit USF recipients from buying equipment based on a determination that a seller allegedly posed a risk to national security. 6/1/2018 Huawei Comments at 12-35. The Communications Act directs the Commission to make USF decisions based only on the enumerated principles set forth in the universal service statute, 47 U.S.C. § 254(b). Those principles center on ensuring that reasonably priced, quality telecommunications and broadband services are available in rural, insular, and high-cost areas. As Huawei explained, those principles do not include national security. *Id.* at 13. And the Commission has no power to unilaterally adopt or rely on a new universal-service principle. *Id.* at 15. Moreover, Congress has expressly empowered the President to consider national security in certain other parts of the communications laws, but conspicuously did not empower the Commission to do so in the context of the USF program. *Id.* at 17-19. If Congress had intended to grant the Commission the politically, diplomatically, and constitutionally significant power to make USF decisions based on national security and foreign policy, it would have done so explicitly. *Id.* at 19-24.

Second, Huawei asserted that the proposed rule was vague and irrational, and thus arbitrary and capricious under the Administrative Procedure Act ("APA"). *Id.* at 35-53. For example, the

Commission's failure in the NPRM to define "national security" or to propose any criteria for deciding which companies to blacklist would render any resulting rule impermissibly vague. The Commission also drew irrational distinctions by targeting specific sellers, apparently based on their national origin, rather than on characteristics of their equipment. *Id.* at 38-39. And the Commission irrationally targeted companies like Huawei because their headquarters are in China, while permitting the use of equipment from other companies that also operate, manufacture, and develop products in China. *Id.* at 40. In so doing, the Commission ignored the realities of telecommunications supply chains. *Id.* at 39.

Third, Huawei argued that the proposed rule's substantial costs outweighed its speculative benefits, such that the Commission lacked a rational basis for the rule. *Id.* at 54-59. As Huawei explained, the benefits of the proposed rule depended on the accuracy with which the Commission could identity threats to U.S. national security. *Id.* at 54. But it was impossible to have confidence in the accuracy of the Commission's national security judgments where the proposed rule failed even to describe the standards or criteria to be used in rendering such judgments, and where the Commission did not propose to conduct an inquiry into the alleged threats itself. *Id.* at 54-55. Moreover, the proposed rule failed to address the complexities of the global supply chain, and as a result would address only a small portion of potential threats. *Id.* at 55. Huawei also explained that the costs of the proposed rule would be substantial because the rule would decrease competition in the U.S. telecommunications market and increase costs for USF recipients and American consumers. *Id.* at 57-59. Huawei also contended that the proposed rule would impede the development of emerging telecommunications technologies like 5G. *Id.* at 58.

Fourth, Huawei stressed that the proposed rule would violate the Fifth Amendment's Due Process Clause, the Communications Act, and the APA by blacklisting companies, and thereby

depriving them of their constitutionally protected liberty and property interests, before providing them with notice and a meaningful opportunity to be heard. *Id.* at 59-85. Huawei also observed that the Due Process Clause prevents the Commission from using rulemaking procedures to single out particular companies as "national security threats." *Id.* at 60. In addition, Huawei argued that the Commission's proposal to define companies as national security risks based on another federal agency's national security–based debarment decisions would violate constitutional and legal limits on giving preclusive effect to earlier agency actions. *Id.* at 83-88.

Finally, Huawei pointed out that the Commission lacked any factual basis to determine that Huawei was a national security threat. *Id.* at 86-91. Rather than engaging with Huawei's longstanding commitment to network security, the Commission prejudged Huawei based on the geographic location of its headquarters and the nationality of its founder. *Id.* at 89. The Commission provided no evidence that Huawei's equipment poses a national security threat, but instead relied on unspecified and unverified allegations—chiefly, those in the HPSCI Report. *Id.* at 87-88. The HPSCI Report, in turn, relied heavily on an interpretation of a now-defunct Chinese law; moreover, as Huawei pointed out in its Comments, the HPSCI's interpretation of that law was flawed. Not only does Chinese law lack any provision authorizing the Chinese government to interfere in private companies' operations, but it also affirmatively protects corporate entities from such government interference. *Id.* at 87-88. In addition, neither the HPSCI nor the Commission identified any evidence that Huawei had engaged in harmful conduct in the past, and they provided no rational, factual basis to suggest that Huawei would do so in the future.

2. On July 2, 2018, Huawei submitted reply comments. Ex. 2, 7/2/2018 Huawei Reply Comments ("7/2/2018 Huawei Reply Comments"). Huawei supported these comments with additional evidence, including, among other things, a number of declarations and expert reports. These

materials included supplemental declarations from Donald Purdy (Ex. 2-A, Reply Declaration of Donald Purdy, Jr. (submitted as Ex. A to 7/2/2018 Huawei Reply Comments) ("7/2/2018 Purdy Supp. Decl.")); Thomas Dowding (Ex. 2-C, Reply Declaration of Thomas Dowding (submitted as Ex. C to 7/2/2018 Huawei Reply Comments) ("7/2/2018 Dowding Supp. Decl.")); and Dr. Allan L. Shampine (Ex. 2-D, Reply Declaration of Allan L. Shampine (submitted as Ex. D to 7/2/2018 Huawei Reply Comments) ("Shampine Supp. Decl.")).

While Huawei's competitors submitted comments in support of the proposed rule, Huawei pointed out that most comments that the Commission received confirmed Huawei's main arguments—*i.e.*, (1) that the FCC lacked statutory authority to promulgate the proposed rule, *id.* at 3-16; (2) that even if the Commission had statutory authority for the rule, the manner in which it proposed to exercise that authority was arbitrary and capricious in multiple respects, *id.* at 18-28; (3) that the costs of the proposed rule vastly outweighed any potential benefits, *id.* at 29-38; (4) that the proposed rule violated the targeted companies' procedural rights, *id.* at 57-61; and (5) that the proposed rule impermissibly relied on unsupported—and unsupportable—factual allegations against Huawei, *id.* at 61-64.

3. On August 6, 2018, Huawei submitted an ex parte filing responding to other parties' reply comments, Ex. 3, 8/6/2018 Huawei Ex Parte, supported by additional evidence, including a declaration from Jihong Chen and Jianwei Fang (Ex. 3-B, Supplemental Declaration of Jihong Chen and Jianwei Fang (submitted as Ex. B to 8/6/2018 Huawei Ex Parte) ("8/6/2018 Chen & Fang Supp. Decl.")); and an expert report from University of Pennsylvania Professor Jacques deLisle, who has more than thirty years of experience researching and teaching about Chinese law and politics (Ex. 3-A, Expert Report of Jacques deLisle (submitted as Ex. A to 8/6/2018 Huawei Ex Parte) ("deLisle Report")).

Huawei argued that, like the initial comments, the weight of the submitted reply comments confirmed that the Commission's proposed blacklist was legally infirm and arbitrary and capricious; that its costs outweighed its benefits; that it suffered from multiple procedural and constitutional defects; and that it lacked any factual support. 8/6/2018 Huawei Ex Parte at 1. Huawei also rebutted the reply comments of the Telecommunications Industry Association ("TIA"), the only reply commenter that tried to defend the Commission's proposal in any detail. *Id.* For example, TIA argued that the proposed rule advanced the universal service principle of "quality services," but Huawei pointed out that TIA's interpretation departed from the plain meaning of the statute and violated numerous canons of statutory interpretation, including that Congress "does not … hide elephants in mouseholes." *Id.* at 5 (quoting *Whitman* v. *Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001)). In addition, TIA argued that the Commission could make national security judgments because doing so would be in the public interest. But Huawei noted that the Supreme Court has "consistently held" that "the words 'public interest' in a regulatory statute" grant an agency the authority only to promote "the purposes of the regulatory legislation." *Id.* at 5 (quoting *NAACP* v. *Fed. Power Comm'n*, 425 U.S. 662, 670 (1976)). The exclusive purposes of the USF legislation are enumerated in 47 U.S.C. § 254(b) and do not include national security. *Id.* Huawei also rebutted TIA's accusations against Huawei, which—in addition to being false, unfounded, and misleading—constituted adjudicative facts that needed to be resolved in a hearing, not a rulemaking proceeding. *Id.* at 47-48.

4. On August 23, 2018, Huawei submitted another ex parte filing, explaining that its products are safe and that they are subject to a robust testing and certification regime. Ex. 4, 8/23/2018 Huawei Ex Parte. Huawei explained that, as one of the most advanced practitioners in

the telecommunications industry for cybersecurity testing and certification, it complies with standard security review processes. *Id.* at 1. In addition, the United Kingdom and Huawei have worked together to adopt a cybersecurity review process for Huawei equipment. *Id.* at 1-2. The UK's "Huawei Cyber Security Evaluation Centre" ("HCSEC") is monitored by a public–private Oversight Board composed of individuals with UK security clearances who evaluate a range of Huawei products deployed in the UK telecommunications market. *Id.* The HCSEC, like other security certification bodies, has never found any malicious code or backdoor in Huawei's products. *Id.* at 4. And Huawei has promptly remediated any technical issues identified by the Oversight Board, thus demonstrating that the UK's collaborative approach is effective and superior to the approach proposed by the Commission. *Id.* at 3-4.

5. On August 27, 2018, Huawei submitted an additional ex parte filing incorporating comments that Huawei had filed before the Federal Trade Commission, which explained that Huawei's presence in the United States aids market diversity and provides significant benefits to U.S. consumers. Ex. 5, 8/27/2018 Huawei Ex Parte. Huawei noted that the benefits of Huawei's presence in the U.S. telecommunications market must be considered in any cost-benefit analysis.

6. On October 1, 2018, Huawei notified the Commission of communications between representatives of Huawei, Huawei's outside counsel, and several Commission staff regarding the NPRM. Ex. 6, 10/1/2018 Huawei Ex Parte. During these meetings, Huawei provided the Commission with background information on its operations as a telecommunications company trusted by customers around the globe. *Id.* at 2. Huawei also urged the Commission to consider the substantial costs of the NPRM. For example, Huawei pointed out that the proposed rule would have a particularly serious impact on carriers in rural and remote areas who purchase Huawei equipment due

to its quality and affordability. *Id.* at 3. Huawei also attempted to correct the Commission's apparent misconception that Huawei's equipment presents security risks. Huawei explained that it promotes best practices in cybersecurity by, for example, establishing and implementing a transparent global assurance program for cybersecurity and privacy. *Id.* at 7.

D. Congress enacts the National Defense Authorization Act for Fiscal Year 2019 ("2019 NDAA") and the Commission seeks and receives comments

While the NPRM was pending, Congress passed and the President signed the 2019 NDAA. *See* Pub. L. No. 115-232, § 889, 132 Stat. 1636 (Aug. 13, 2018). That legislation imposed restrictions on executive agencies' ability to procure certain Huawei equipment or services for particular uses, and restricted those agencies' ability to contract with entities that used certain Huawei equipment or services for certain purposes. It also prohibited use of federal loan and grant funds to purchase certain Huawei equipment and services. The 2019 NDAA marked yet another step in Congress' wholescale attack on Huawei. During a speech on the Senate floor, Senator Cotton told his fellow legislators that Huawei and ZTE had "proven themselves to be untrustworthy," and that "the only fitting punishment would be to give them the death penalty; that is, to put them out of business in the United States." 164 Cong. Rec. 98, at S3896 (June 13, 2018). The sponsors of this law—including Senator Cotton—were among those who signed the December 20, 2017, letter to Chairman Pai that prompted the proposed rule. *See supra* pp. 8-9.[3]

Soon after the 2019 NDAA's enactment, the Wireline Competition Bureau issued a Public Notice seeking further comment on how the 2019 NDAA "might apply to support provided by the USF." *Wireline Competition Bureau Seeks Comment on Section 889 of John S. McCain Nat'l Def.*

[3] Huawei's constitutional challenge to provisions of section 889 of the 2019 NDAA is pending in federal district court. *See Huawei Techs. USA, Inc., et al.* v. *United States, et al.*, No. 4:19-cv-00159-ALM (E.D. Tex. filed Mar. 6, 2019).

Authorization Act for Fiscal Year 2019, Public Notice, 33 FCC Rcd. 10183 (Oct. 26, 2018). This Notice again failed to provide any standard by which companies might be adjudicated a national security threat under the Commission's proposed rule. And nowhere did the Public Notice indicate that the Commission would designate specific companies under the rule at the same time it announced the rule's adoption.

On November 16, 2018, Huawei submitted comments addressing section 889 of the 2019 NDAA. Ex. 7, 11/16/2018 Huawei Comments. Huawei asserted that section 889 did not have any effect on the proposed rule because section 889 applies only to procurement of certain equipment and services by federal executive agencies and recipients of federal "loan or grant" funds, and use of certain Huawei equipment by federal contractors. Therefore, by its own terms, section 889 does not apply to recipients of subsidies such as universal service support. *Id.* at 3-12. In addition, Huawei argued that section 889 could not sustain the Commission's proposal for the additional reason that the Commission's proposal (which covers all equipment) was significantly broader than section 889 (which covers only the use of "telecommunications equipment" "as substantial or essential component" of any system, or "as critical technology" as part of any system, and exempts equipment that cannot route or redirect user data, or permit visibility into user data). *Id.* at 12-13. Finally, Huawei contended that the Commission may not declare a company a threat to national security simply because Congress imposed restrictions on that company's products in the 2019 NDAA. Huawei explained that (1) treating an existing statute as a substitute for a hearing would deny Huawei due process; (2) the Commission cannot rationally rely on a statute to prohibit transactions that are beyond the scope of the statute; and (3) it would be arbitrary and capricious to assume that statutory restrictions on the use of certain categories of Huawei's equipment in

particular situations means that all of Huawei's equipment is threatening in entirely different circumstances. *Id.* at 18-19.

On December 7, 2018, Huawei submitted reply comments observing that the few commenters that took the opposing view ignored the plain language and structure of section 889. Ex. 8, 12/7/2018 Huawei Reply Comments. And on January 28, 2019, Huawei submitted an ex parte filing responding to the TIA's extreme, unreasonable, and atextual arguments for the applicability of section 889(b)(1). Ex. 9, 1/28/2019 Huawei Ex Parte.

E. Huawei submits additional ex parte filings

On February 15, 2019, while awaiting further action from the Commission on the proposed rule, Huawei submitted an ex parte filing to address the Supply Chain Security Act, which requires the development of government-wide criteria and rules for identifying, assessing, and mitigating supply chain risks posed by any global supplier. Ex. 10, 2/15/2019 Huawei Ex Parte. Huawei applauded the law because it allows government officials with national security expertise to evaluate and respond to risks across the entire global supply chain, rather than blacklisting a handful of companies based on their national origin. *Id.* at 1-2. The Act also provides meaningful safeguards and due process protections to promote accurate and equitable results, including notice, opportunity for rebuttal, and judicial review. *Id.* at 1. Huawei argued that the Commission should abandon its rulemaking proceeding in favor of the superior processes established by the Act. *Id.* at 2.

On March 12, 2019, in another ex parte filing, Huawei urged the Commission to promote the immediate deployment of the most advanced mobile technology to as many Americans as possible. Ex. 11, 3/12/2019 Huawei Ex Parte. Huawei emphasized its readiness to compete with other telecommunications companies to build secure 5G networks in the United States. *Id.* at 3. In addition, Huawei shared the complaint that it had filed in federal court on March 6, 2019, challenging

the constitutionality of section 889 of the NDAA. *Id.* at 2; Ex. 11-A, Complaint, *Huawei Technologies USA, Inc. et al.* v. *United States*, No. 4:19-cv-00159-ALM (E.D. Tex.) (submitted as Ex. A to 3/12/2019 Huawei Ex Parte).

On May 10, 2019, Huawei submitted an ex parte filing to refute the Commission's—and the HPSCI Report's—flawed interpretation of Chinese law. Ex. 12, 5/10/2019 Huawei Ex Parte. This filing included an expert report from Dr. Hanhua Zhou, who serves as the Executive Vice President and Secretary General of the Cyber and Information Law Research Committee of China Law Society. Ex. 12-A, Expert Report of Dr. Hanhua Zhou (submitted as Ex. A to 5/10/2019 Huawei Ex Parte) ("5/10/2019 Zhou Report"). In his report, Dr. Zhou clarified that any support, assistance, and cooperation obligations imposed on corporate entities by Chinese law are strictly defensive and limited in scope by the Chinese Constitution. *Id.* at 1; 5/10/2019 Zhou Report. Dr. Zhou provided a detailed analysis of the National Intelligence Law ("NIL"), Cyberespionage Law, Counterterrorism Law, and Cybersecurity Law. 5/10/2019 Ex Parte at 1. After providing the legislative history, purpose, and context of these laws, Dr. Zhou attempted to correct the Commission's apparent misconceptions, including its assertion that Chinese national intelligence agencies could require Huawei to implant "backdoors" in its equipment, facilitate cyberespionage, or otherwise harm the communications networks of other countries. *Id.* at 2. He also pointed out that other laws in China, including the Cyber Security Law, affirmatively prohibit companies from "endangering cybersecurity" or "interfering with the normal functions of others' networks and stealing cyber data." *Id.* at 2. In addition to its submission of the Zhou Report, Huawei notified the Commission of several recent statements by Chinese officials reiterating that the Chinese government does not request—and Chinese law does not require—telecommunications companies to install backdoors or collect foreign intelligence. *Id.* at 3.

On June 12, 2019, Huawei filed another ex parte submission, in which it reasserted that banning specific vendors on alleged "national security" grounds would do little or nothing to protect the security of America's telecommunications networks. Ex. 13, 6/12/2019 Huawei Ex Parte. Huawei brought to the Commission's attention statements by Susan Gordon, Principal Deputy Director of National Intelligence, conceding that targeting specific vendors is neither necessary nor sufficient to ensure network stability. *Id.* at 4. Huawei also raised other statements by U.S. officials encouraging the adoption of a holistic approach that is "country and company agnostic." *Id.* at 5. Further, Huawei summarized the approaches adopted by Germany, France, and Canada, all of which use generally applicable security and testing requirements for 5G equipment that do not single out specific companies to exclude from the market. *Id.* at 6-7. Finally, Huawei asserted that imposing an equipment ban based on county of origin would likely violate the anti-discrimination obligations imposed on all members of the World Trade Organization and the General Agreement on Tariffs and Trade. *Id.* at 8-9.

On September 18, 2019, Huawei filed a further ex parte submission to supplement the record with additional publicly available facts about Huawei's competitors that demonstrated that these companies have connections to China that are equal to, or stronger than, Huawei's alleged connections. Ex. 14, 9/18/2019 Huawei Ex Parte. For example, unlike Huawei, several of its competitors are owned by the Chinese state. *Id.* at 1. Huawei made this submission not to argue that these companies should be targeted under the proposed rule due to their close ties to the Chinese government, but rather to show that that the proposed rule was arbitrary in its application to certain companies and not others. *Id.* at 3-4.

On October 11, 2019, Huawei filed an additional ex parte submission with supporting evidence, including an expert report from Dr. Debra J. Aron of Charles River Associates, an economist specializing in economic analysis and policy in the telecommunications industry. Ex. 15, 10/11/2019 Huawei Ex Parte; Ex. 15-A, Expert Report of Dr. Debra J. Aron (submitted as Attach. 1 to 10/11/2019 Huawei Ex Parte) ("Aron Report I"). Dr. Aron concluded that Huawei's exclusion would likely delay 5G deployment, depress competition, and reduce job availability for U.S. workers. Aron Report I ¶ 11-22.

F. Ex parte contacts between Huawei's competitors and the Commission

After the Commission released its NPRM, but before it issued its final rule—*i.e.*, during the period when the Commission was engaged in an unannounced adjudication of Huawei—some of Huawei's direct competitors engaged in ex parte contacts with the Commission. For example, on May 18, 2018, key executives and legal counsel from Nokia met with Chairman Pai, Commissioner O'Rielly, and Commissioner Rosenworcel. *See* 5/22/2018 Nokia Ex Parte. Although transcripts of these meetings were not included in the record, "the Nokia Executives advocated on key proceedings before the Commission." *Id.* at 1. Nokia stated that it "supported" the proposal that USF funds "not be used to purchase equipment that is a threat to national security," but also "urged that the proceeding not be used to cast uncertainty on the entire industry, including longstanding, well-vetted partners of U.S. government and industry, like Nokia." *Id.* at 2.

On August 28, 2018, Nokia had additional ex parte contacts with Commissioners O'Rielly and Rosenworcel; on August 29, 2018, with a legal advisor to Commissioner Carr; and on August 30, 2018, with special counsel to Chairman Pai. *See* 8/30/2019 Nokia Ex Parte. Again, the record contains no transcript of these contacts, but the description of these meetings indicates that they included discussions of the "emerging headwinds, that are mostly external to Commission jurisdiction, that nevertheless threaten to impede 5G roll-out." *Id.* at 1. The descriptions also indicate

that Nokia responded to what it called "a number of absurd claims made by Huawei" in the USF proceedings. *Id.* at 1-2.

During the week of June 24, 2019, Nokia representatives met with Chairman Pai's international advisor, as well as Commissioners O'Rielly, Carr, and Starks, regarding a "wide range of issues that are priorities for Nokia." 6/27/2019 Nokia Ex Parte. Although the record again contains no transcripts, Nokia stated that it "provided a briefing on Nokia's advisory role to multiple officials and agencies in the U.S. government on how to secure 5G networks, offering technical assistance to the Commission as it continues to address this difficult issue." *Id.* at 2. Then, on July 25, 2019, Nokia representatives met with Commissioner Rosenworcel to discuss "several issues that are priorities for Nokia." 7/29/2019 Nokia Ex Parte. This contact also included a briefing "on how to secure 5G networks" and "offering technical assistance to the Commission." *Id.* at 1.

G. Three Commissioners publicly reveal their prejudgment that Huawei is a national security threat

Before issuing the rule and designating Huawei under it, several Commissioners publicly revealed their views that Huawei poses a national security threat. For example, during a hearing on May 7, 2019, Chairman Pai told the Senate Subcommittee on Appropriations: "I believe that certain Chinese suppliers, such as Huawei, do indeed present a threat to the United States, either on their own or because of Chinese domestic law." Ex. T, John Eggerton, *FCC's Pai to Senate: Huawei is National Security Threat*, Broadcasting+Cable (May 8, 2019). Similarly, on October 28, 2019, Commissioner Brendan Carr tweeted a *Wall Street Journal* article by Chairman Pai entitled "FCC Answers The Threat From Huawei" and commented: "I have no doubt that China intends to spy on persons and businesses within our borders. We must secure our telecom networks from this threat. I'm glad we're acting on the rip and replace proposal that I first discussed last year." Ex. W, Brendan Carr (@BrendanCarrFCC), Twitter (Oct. 28, 2019, 12:34 PM).

Commissioner Geoffrey Starks also made numerous public statements that revealed his firm position that he believes Huawei poses a national security threat. For example, on May 26, 2019, Commissioner Starks wrote an article asserting that "Huawei's equipment contains software vulnerabilities that could seriously compromise our network security," and that "[t]he Federal Communications Commission must find this equipment and work with other policymakers to fix the security problems and fund a solution for affected carriers." Ex. X, Geoffrey Starks, *The Huawei threat is already here*, TheHill (May 26, 2019) ("Starks, *The Huawei threat is already here*"). When asked in an interview whether there was anything Huawei could do to earn Commissioner Starks' trust or otherwise remedy the situation, Commissioner Starks stated that it would be "very hard" for Huawei "to mitigate" these issues. Ex. Y, Nilay Patel & Makena Kelly, *FCC Commissioner Geoffrey Starks talks Huawei and net neutrality on The Vergecast*, TheVerge.com (May 21, 2019) ("Patel & Kelly, *FCC Commissioner Geoffrey Starks talks Huawei and net neutrality on the Vergecast*"). And on June 22, 2019, Commissioner Starks stated: "The thing that I'm really focused on right now is coming up with solutions for dealing with Huawei and other risky equipment that's already in our networks." Ex. Z, Marguerite Reardon, *FCC commissioner wants Huawei gear out of US networks*, CNET (Jun. 22, 2019) ("Reardon, *FCC commissioner wants Huawei gear out of US networks*").

H. The Commission releases a Draft Report and Order

On October 29, 2019, the Commission released a Draft Report and Order. Like the NPRM, the Draft Report and Order offered no definitions or criteria for understanding what it means to "pos[e] a national security threat to the integrity of communications networks or the communications supply chain." Draft Report and Order at 56 (codified at 47 C.F.R. § 54.9(a)). And, although the Commission in the NPRM proposed three "approach[es]" for making such a determination (albeit approaches without any apparent standard), *id*. ¶¶ 19-22, the Draft Report and Order made

no attempt to articulate even a semblance of an "approach" or standard. Also like the NPRM, the Draft Report and Order made clear that the purportedly general rule is a poorly disguised mechanism for imposing a targeted ban on Huawei and ZTE. Indeed, the Commission's cost-benefit analysis took into account *only* the costs associated with banning USF recipients from using Huawei and ZTE equipment, thus reflecting the Commission's foregone conclusion that Huawei and ZTE should be designated regardless of the designation procedures that might follow.

The text of the Draft Report and Order also confirmed that pressure from members of Congress had shaped the Commission's decision to enact a rule targeting Huawei. The Draft Report and Order explicitly cited congressional communications that the Commission received regarding Huawei. *See, e.g.*, Draft Report and Order ¶ 6 (October 2010 letter from lawmakers to the FCC Chairman expressing concern about Huawei); *id.* ¶ 11 (December 2017 letter from eighteen Senators and Representatives to Chairman Pai regarding Huawei). It also repeatedly cites the HPSCI Report. *See, e.g.*, *id*. ¶¶ 7, 11. And it explicitly cites section 889 of the 2019 NDAA as a basis for the rule and for its decision to target Huawei, stating that section 889 expresses Congress's view that "the role of the Commission … is to prevent the use of federal funds under [its] control on equipment and services from … suppliers of concern," and explaining that its rule and "initial designation of Huawei" were "consistent" with that congressional view. *Id.* ¶ 37 (quotation marks omitted).

In other important respects, however, the Draft Report and Order departed markedly from the NPRM. Perhaps most notably, the Draft Report and Order immediately, and without notice, announced that the Commission would "[i]nitially designate Huawei Technologies Company and ZTE Corporation as covered companies" for allegedly "pos[ing] a threat to the security of com-

munications networks or the communications supply chain." *Id* ¶ 27. The Commission also proposed an additional new rule that would require all USF recipients "to remove existing equipment and services produced or provided by covered companies"—namely, Huawei and ZTE—from their networks. *Id.*

The congressional delegation that had sought to target and destroy Huawei's U.S. operations applauded the Commission's action. And in the Draft Report and Order's immediate aftermath, Attorney General William P. Barr wrote a letter to Chairman Pai "strongly encourag[ing]" the Commission to finalize its initial designation of Huawei and "launch … a process to remove and replace" the company's equipment. Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, FCC, WC Docket No. 18-89, at 2 (Nov. 13, 2019) ("Barr Letter").

I. Huawei responds to the Draft Report and Order

Huawei submitted several ex parte filings responding to the Draft Report and Order and its unexpected new approach.

1. On October 31, 2019, Huawei filed an ex parte submission to point out the flaws in the Draft Report and Order's reliance on a report by Finite State (the "Finite State Report"), which purported to assess the security of Huawei's products and services. Huawei attached copies of its previous responses to the Finite State Report and summarized its multiple errors. Ex. 16, 10/31/2019 Huawei Ex Parte at 2. As Huawei explained, the Finite State Report evaluated outdated versions of Huawei's products and identified issues that had been already fixed in new versions. *Id*. Further, the Finite State Report based some of its conclusions on the mistaken assumption that Huawei used standard Linux-based authentication. *Id.* In addition, Finite State failed to adhere to general practices of responsible security testing, which typically involve dialogue between the security company and vendor about alleged vulnerabilities to ensure a complete and accurate assessment of vulnerabilities. *Id.* Huawei criticized the Draft Report and Order for accepting the Finite

State Report's conclusions at face value without any assessment of its methodology or the accuracy of its assertions. *Id.* at 3.

2. On November 1, 2019, Huawei filed an ex parte submission that proffered an expert report from Dr. Valtteri Niemi, Deputy Head of the Computer Science Department at the University of Helsinki and an expert on secure systems and mobile communications security. Ex. 18, 11/1/2019 Huawei Ex Parte; Ex. 18-A, Expert Report of Professor Valtteri Niemi (submitted as Attach. 1 to 11/1/2019 Huawei Ex Parte) ("Niemi Report"). Professor Niemi discussed the enhanced security requirements and features that are automatically built into 5G networks. 11/1/2019 Huawei Ex Parte. Huawei argued that the Commission failed to carefully weigh the benefit of enhanced security that would necessarily accompany faster 5G deployment. Professor Niemi's expert report bolstered Huawei's argument that the USF rule is arbitrary and capricious because the Commission's cost-benefit analysis is woefully deficient. *Id.* at 1-2.

3. Also on November 1, 2019, Huawei filed an ex parte submission with supporting evidence that included a supplemental expert report from Dr. Hanhua Zhou, Executive Vice President and Secretary General of the Cyber and Information Law Research Committee of China Law Society and an expert on China's National Intelligence Law. Ex. 17, 11/1/2019 Huawei Ex Parte; 17-A, Supplemental Expert Report of Dr. Hanhua Zhou (submitted as Attach. A to 11/1/2019 Huawei Ex Parte) ("11/1/2019 Zhou Supp. Report"). Dr. Zhou clarified that Article 17 of China's National Intelligence Law does not, as the Commission alleged, allow Chinese intelligence agencies to take control of an organization's communications equipment. 11/1/2019 Huawei Ex Parte at 2. Rather, Dr. Zhou explained, Article 17 provides only that the staff of national intelligence agencies have preferential use of communications tools and does not impose any requirement on third parties. *Id.* at 3. Moreover, Article 17 is applicable only in the geographic territory of China.

Nothing in Article 17 allows Chinese intelligence officials to access Huawei's telecommunications facilities, much less its telecommunications facilities in carriers' networks in the United States. *Id*. Finally, Dr. Zhou's Report further clarified that Article 17 is a defensive measure and does not provide authority for Chinese intelligence agencies to engage in offensive intelligence activities. *Id.* at 3-4.

4. On November 8, 2019, Huawei filed an ex parte submission with supporting evidence, including a rebuttal memorandum from Jihong Chen. Ex. 19, 11/8/2019 Huawei Ex Parte; Ex. 19-A, Jihong Chen Rebuttal to Donald Clarke's Memorandum (submitted as Attach. A to 11/8/2019 Huawei Ex Parte) ("Chen Rebuttal to Clarke Memo"). Mr. Jihong Chen rebutted the erroneous conclusions of the self-published "expert" report of Donald C. Clarke. 11/8/2019 Huawei Ex Parte at 2. Huawei sought to correct the Commission's misconceptions about the relationship between Huawei's U.S. subsidiaries and the Chinese government. *Id.* at 1.

5. On November 12, 2019, Huawei filed an ex parte submission responding to the Commission's assertion that "several of the United States' closest allies have concluded that the risk posed by Huawei equipment and systems is too great to bear." Draft Report and Order ¶ 50. To the contrary, Huawei explained, U.S. allies use Huawei in their networks, and much of Europe, Africa, the Middle East, and the Americas plan to deploy 5G networks with certain Huawei equipment. Ex. 20, 11/12/2019 Huawei Ex Parte at 2-3. In addition, the Draft Report and Order purported to rely on the European Union's ("EU's") Coordinated Risk Assessment of the Cybersecurity of 5G Networks as evidence of international support for its draft rule, but that EU risk assessment advocates for the adoption of a holistic cybersecurity approach that is based on a true risk assessment methodology rather than a blanket, country-of-origin ban like that announced in the

Draft Report and Order. *Id.* at 4. Moreover, none of the EU member states have plans to exclude Huawei, and many have publicly declared that they will not do so. *Id.*

6. On November 14, 2019, Huawei filed a final ex parte submission. Huawei began by responding to the Commission's eleventh-hour proposal to rely on the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1004, as a source of statutory authority for the USF rule. *First*, Huawei asserted that the Commission could not rely on CALEA because it never proposed to rely on CALEA in its NPRM. Thus, a rule based on CALEA would not be a logical outgrowth of the proposed rule. Ex. 21, 11/14/2019 Huawei Ex Parte at 2-3. *Second*, Huawei explained that the Commission's proposed interpretation of CALEA ignored the statute's plain text, context, and legislative history. Section 1004, on which the Commission purported to rely, imposes obligations on carriers to safeguard their networks from unauthorized interceptions "effected within [the carrier's] switching premises" by domestic law enforcement. Thus, § 1004 does not reach beyond a carrier's "switching premises" to combat interceptions by foreign adversaries. *Id.* at 4-5. CALEA therefore cannot sustain a rule that prohibits USF recipients from purchasing all equipment of a covered entity for use anywhere in the carrier's network, especially because not all points or equipment in a carrier's network engage in switching. *Id.* at 4-5. *Third*, Huawei pointed out that CALEA applies only to providers of telecommunications services, so CALEA cannot not sustain a rule that covers entities excluded from the scope of CALEA, including providers of private networks. *Id.* at 6 & n.25. *Fourth*, CALEA is a generally applicable statute; it does not grant the Commission any rulemaking authority specific to the USF context. *Id.* at 6. It would thus be irrational to impose a rule under CALEA on just a subset of carriers because CALEA by its very terms applies to all telecommunications carriers. *Id.*

In addition to identifying the flaws in the Commission's reliance on CALEA, Huawei's ex parte submission argued that the draft rule and proposed designation proceeding were unlawful for several additional reasons, including:

- The draft rule is not a logical outgrowth of the proposed rule insofar as it relies on the invocation of "public safety" under 47 U.S.C. § 254(c)(1)(A). And, in any event, the Commission is wrong on the merits because § 254(c)(1)(A) cannot sustain the rule.

- Neither the designation process, nor the adjudication of Huawei under the newly adopted rule, is a logical outgrowth of the proposed rule. The Commission did not propose a process for designating companies a national security threat in the NPRM, yet it now purports to create and apply such a process with no notice or opportunity for comment.

- If the draft rule contains any ascertainable criteria for determining whether "a company poses a national security threat," those criteria did not appear in the NPRM and are not a logical outgrowth of the proposed rule. Moreover, since the draft rule in fact fails to state meaningful and ascertainable criteria, the rule is vague and standardless. The draft rule gives companies no way of knowing what is required to avoid designation and provides no guidance to prevent arbitrary or discriminatory enforcement.

- The Commission's draft rule is impermissibly retroactive. With no prior notice, the Draft Report and Order simultaneously announced a new rule and designated Huawei pursuant to that rule based on alleged pre-promulgation conduct and associations. The draft rule is thus invalid as a "rule" and is "arbitrary and capricious."

- The draft rule is arbitrary and capricious because, among other things, it fails to address many material comments and proposed alternatives submitted by Huawei and other parties.

- The Commission's decision to convert the proceeding from a rulemaking—the only type of proceeding contemplated by the Notice of Proposed *Rulemaking*—to a rulemaking plus an adjudicatory decision (*i.e.*, Huawei's initial designation) was unlawful and prejudicial. The Commission's combination of rulemaking and adjudication in a single hybrid proceeding is contrary to fundamental principles of administrative and constitutional law as guaranteed by the text and structure of the APA. In addition, the Commission's designation denied Huawei the notice and opportunity for comment guaranteed by the APA and Constitution; and the draft rule neither defined what it means to be a "national security threat" nor established criteria that the Commission will follow in applying the proposed rule. As a result, Huawei has been deprived of any opportunity to know what criteria the Commission is relying on, or the standards against which any rebuttal or response will be measured, much less to address the Commission's purported "facts" or underlying reasoning. In addition, Huawei had no opportunity to address the harm that such an initial designation will cause to its reputation and business goodwill.

- The proposed rule provided no notice regarding what procedural protections the Commission intended to afford initially designated companies, and the Draft Report and Order provided for nothing more than the opportunity to submit written comments. These minimal procedures afforded in the *rulemaking* process are plainly insufficient to protect the constitutional interests at stake in these *adjudicatory* proceedings. The Commission's failure to provide sufficient procedural protections was based in part on its misunderstanding of the liberty and property interests at issue. Although Huawei explained in its prior submissions that it is entitled to the full panoply of protections guaranteed by the Due Process Clause of the Fifth Amendment and the formal adjudication provisions of the APA and Communications Act, *see* 6/1/2018 Huawei Comments at 61-86, the Commission improperly rejected this argument in the Draft Report and Order. But even if the Commission were to deny Huawei these required protections, it is still obligated to provide prompt and transparent guidance on the designation procedures and to indicate with particularity what process will be afforded, for example, to resolve disputed factual issues.

- The designation process that the Commission proposed is invalid because, among other things, neither the Chief of the Bureau nor any of the Bureau's staff who are responsible for making final designations are properly appointed officers of the United States in accordance with the Appointments Clause of the U.S. Constitution. *See* U.S. Const. art. II, § 2, cl. 2; *see generally Lucia* v. *SEC*, 138 S. Ct. 2044, 2051-55 (2018); *Free Enter. Fund* v. *Pub. Co. Accounting Oversight Bd.*, 561 U.S. 477, 511-12 (2010).

- Even assuming that an independent agency may constitutionally make national security judgments, the non-delegation doctrine forbids Congress from conferring anything more than gap-filling authority on an agency when it delegates lawmaking power, especially on a policy matter as significant as national security. *See Panama Ref. Co.* v. *Ryan*, 293 U.S. 388, 426 (1935); *Gundy* v. *United States*, 139 S. Ct. 2116, 2136-39 (2019) (Gorsuch, J., joined by Roberts, C.J., and Thomas, J., dissenting); *id*. at 2130-31 (Alito, J., concurring in the judgment). At a bare minimum, Congress must provide an intelligible principle to guide the agency's actions. *Whitman*, 531 U.S. at 472. Consequently, under interpretive principles of constitutional avoidance, the Commission may not read 47 U.S.C. § 254 (or any other statute) to give it the power to place restrictions on USF funds in the name of national security. *See, e.g., Nat'l Cable Television Ass'n, Inc.* v. *United States*, 415 U.S. 336, 342 (1974) ("[T]he hurdles revealed in [the Supreme Court's non-delegation] decisions lead us to read the Act narrowly to avoid constitutional problems" regarding Congress' delegation of taxing authority to the FCC); *Indus. Union Dep't* v. *Am. Petroleum Inst.*, 448 U.S. 607, 646 (1980) (plurality opinion) (construing statute to render an agency's interpretation of the statute void in order to avoid a constitutional non-delegation question); *Indus. Union Dep't*, 448 U.S. at 672-76 (Rehnquist, J., concurring in the judgment).

J. The Commission releases its Final Report and Order

On November 22, 2019, despite Huawei's arguments, the Commission published its Final Report and Order, which largely mirrored the draft. The Order formally adopted a rule prohibiting

the use of USF funds to purchase equipment or services from any entity that the Commission designates as a "national security threat to the integrity of communications networks or … supply chain[s]." Order at 66 (codified at 47 C.F.R. § 54.9(a)). The Order did not improve on the cost-benefit analysis in the Draft Report and Order; the final rule plainly targeted Huawei and ZTE and relied on a cost-benefit analysis that focused exclusively on the supposed costs and benefits of removing Huawei and ZTE from the USF program. *Id.* ¶¶ 108-21.

The Order vaguely outlined a process, involving initial and final "designation" proceedings, for determining whether a company presents a "national security threat[]." *Id.* ¶ 39. The Order also provided that the Commission or Bureau may reverse a designation. *Id.* ¶ 42. But the Order adopted no standard or criteria for making—or withdrawing—designations, even though the NPRM had sought comments on the approach the Commission should adopt, and Huawei had urged the Commission to remedy the Draft Report and Order's omission of criteria and standards. The Order also failed to specify what the challenging party must establish, and by what burden of proof, to convince the Bureau that it was wrong to initially designate the company or reverse a final designation. Further, the rule's "procedures" failed to provide for procedural safeguards required by the APA and Constitution before designation. For example, the designation procedures do not entitle a designated company to cross-examine the witnesses against it. They also do not foreclose ex parte contacts, like those that were made between Huawei's direct competitor, Nokia, and the Commission in the months leading up to the publication of the Order. *See, e.g.*, *id.* ¶ 73 n.218.

Finally, the Order initially designated Huawei and ZTE under the rule, despite having provided no notice that Huawei was a party to an adjudication (rather than an interested commenter

to a rulemaking proceeding). The Order reiterated the Commission's "confiden[ce] that the national security risk to our communications networks from permitting Huawei equipment and services is significant." *Id.* ¶ 54. The Commission did not designate any other entities or explain why it did not designate any other entities, despite the extensive information Huawei had submitted about other telecommunications companies' operations in China.

While the rule and procedures adopted in the Order are framed in general terms, the text of the Order makes clear that, like the NPRM, they are designed to target Huawei and ZTE at the behest of members of Congress. For example, the Commission's cost-benefit analysis takes into account *only* the costs associated with preventing carriers from using Huawei and ZTE equipment, *id*. ¶¶ 108-21—an implicit concession that the "rule" is, in reality, only a mechanism for imposing a targeted ban on use of Huawei and ZTE equipment.

The Order also candidly concedes that, while section 889 of the 2019 NDAA does not purport to authorize the Commission's Order, *see id*. ¶ 38 & n.114, the "goals underlying section 889 … support [the Commission's] decision to take action here," because that section "expresses a view that 'the role of the Commission and other executive agencies is to prevent the use of federal funds under their control on equipment and services from [the five] suppliers of concern'" identified in the NDAA, which included Huawei and ZTE, *id*. ¶ 38 & n.117 (quoting 11/16/2018 TIA PN Comments, WC Docket No. 18-89, at 15-16 (Nov. 16, 2018)).

Notably, even though the Order directs the Bureau to make both initial and final designations of entities that supposedly present a threat, the Commission itself made initial designations of Huawei and ZTE. Those actions eliminated all doubt about whether Huawei would be finally designated, immediately injured Huawei's reputation, and answered the congressional call for an agency-imposed boycott of Huawei. Notably, the Commission rested its designation of Huawei in

significant part upon the HPSCI Report and the 2019 NDAA. *See id*. ¶¶ 46, 48, 53-54. In short, rather than acting generally and prospectively, as it was required to do, the Commission created a standardless regime and applied that regime retroactively to Huawei without the legally required process or any legal or factual support.

On January 3, 2020, the Commission published a summary of the Report and Order in the Federal Register. *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation*, 85 Fed. Reg. 230 (Jan. 3, 2020). That publication initiated the 30-day comment period for the designation proceedings before the Bureau.

ARGUMENT

The foregoing procedural history forms an important part of the record in this proceeding. To be sure, both the rule and the initial designation—in which the Commission, the final decisionmaker in these proceedings, announced its "confident" conclusion that Huawei represents a "national security risk to our communications network," Order ¶ 54—represent fully completed, unlawful agency actions that have concretely harmed Huawei and are subject to immediate challenge in court. *See Huawei Techs. USA, Inc.* v. *FCC*, No. 19-60896 (5th Cir. filed Dec. 4, 2019, and Jan. 6, 2020). Even assuming the Commission had statutory authority for the rule and its designation (and that the Bureau, too, has statutory authority to render a final designation), the legal errors the Commission made in promulgating the rule and issuing its designation also infect and render invalid any final designation entered by the Bureau. Any one of these errors or defects would thus be a sufficient basis for the Bureau to decline to enter a final designation.

But the Bureau cannot and should not enter a final designation as to Huawei for at least three additional reasons. *First*, the Commission's initial designation cannot form the basis for a

valid final designation of Huawei, because it is unsupported by sufficient evidence; improperly relies on nonevidence and unreliable evidence and unsupported conclusions about Chinese law; arbitrarily and capriciously treats Huawei differently from other similarly situated telecommunications companies; and is infected by unconstitutional congressional pressure and prejudgment against Huawei. *Second*, additional evidence that Huawei has submitted further demonstrates that final designation of Huawei would be improper. *Third*, and in any event, the Bureau cannot lawfully enter a final designation as to Huawei without providing it with additional legally required procedural safeguards, and unless the decisionmaker is appointed in conformity with the Constitution's Appointments Clause.

I. The existing record and prior proceedings do not support the designation of Huawei as a national security threat to the integrity of communications networks and the communications supply chain

Although the Commission presumably expects its initial designation to dictate the Bureau's final designation, the Bureau cannot lawfully rely on the initial designation to enter any final designation against Huawei. The initial designation was not supported by reliable evidence in the record—where any evidence supported it at all—and it relied on a misunderstanding of Chinese law that constitutes legal error. Further, the initial designation was arbitrary and capricious, and therefore unlawful, because it failed to treat similarly situated companies similarly. In addition, the initial designation was the product of irrational and unconstitutional prejudgment against Huawei.

A. The initial designation was not supported by sufficient evidence in the record

The Commission was required to look to the whole record before it and to prove by a preponderance of the evidence, uninfected by legal error, that designation of Huawei was warranted. During the rulemaking proceedings, Huawei submitted extensive evidence showing that it

and its products are reliable and safe and that it is not a national security threat. But the Commission ignored this evidence. The Commission instead looked to nonevidence and wholly unreliable evidence—from statutes and indictments to the unsubstantiated HPSCI Report by members of Congress more interested in political grandstanding than developing facts—to conclude that Huawei somehow presented a national security threat to the integrity of communications networks and the communications supply chain. Even when these errors are put aside, the Commission's remaining factual conclusions are unsupported by evidence in the record and do not show that Huawei presents a national security threat.

1. The Commission was required to justify its initial designation by a preponderance of the evidence that is actual and reliable and based on the whole record

Two overarching legal standards applied to the Commission's initial designation determination. *First*, the Commission bore the burden of showing that the initial designation was warranted based on a preponderance of the evidence in the record as a whole. *Second*, in making that assessment, the Commission was required to rely upon reliable evidence, not speculation, rumor, or other forms of nonevidence or unreliable evidence. *Third*, the Commission's decision must be free from legal error.

a. The Commission bore the burden of proving by a preponderance of the evidence that its designation of Huawei was warranted

"Absent statutory requirements to the contrary or factors warranting a heightened standard," the Commission bears the burden of showing designation is warranted by a "preponderance of the evidence." *In re Universal Serv. Contribution Methodology*, 29 FCC Rcd. 9715, 9719-20 (2014). Proof by a preponderance of the evidence "is the traditional standard" for both informal and formal administrative adjudications, and the Commission and Bureau carry the burden of proof as the "proponent[s]" of the designation. *Sea Island Broad. Corp.* v. *FCC*, 627 F.2d 240, 243-44

(D.C. Cir. 1980); *see Bender* v. *Clark*, 744 F.2d 1424, 1429 (10th Cir. 1984); *In re Universal Serv. Contribution Methodology*, 29 FCC Rcd. at 9720 n.35; *see also* 5 U.S.C. § 556(d); *Verizon* v. *FCC*, 770 F.3d 961, 967 n.7 (D.C. Cir. 2014).[4]

In making its case, the Commission was required to consider the whole record and address evidence contrary to its conclusions. *See, e.g.*, Order ¶ 41 ("The Commission will base its determination on the totality of evidence …."); 5 U.S.C. § 556(d); *Allentown Mack Sales & Serv., Inc.* v. *NLRB*, 522 U.S. 359, 366 (1998); *AT&T Corp.* v. *FCC*, 86 F.3d 242, 247 (D.C. Cir. 1996) ("The substantiality of evidence must take into account whatever in the record fairly detracts from its weight.") (quoting *Universal Camera Corp.* v. *NLRB*, 340 U.S. 474, 488 (1951)). "[A]n agency cannot ignore evidence contradicting its position." *Butte County* v. *Hogen*, 613 F.3d 190, 194 (D.C. Cir. 2010). The Commission was required to explain "the evidence which is available" and "offer a rational connection between the facts found and the choice made." *Motor Vehicle Mfrs. Ass'n* v. *State Farm Mut. Auto Ins. Co.*, 463 U.S. 29, 52 (1983) (quotation marks omitted).

b. The Commission was required to rely on evidence that is reliable and probative

To carry its burden of showing that designation is supported by a preponderance of the evidence, the Commission was required to rely on evidence—and that evidence must be reliable and probative. The Commission itself has recognized that, when finding facts, it must rely only on

[4] A higher, "clear and convincing evidence" standard applies when "prescribed by statute or where other countervailing factors warrant [such] a higher standard." *In re Am. Commc'ns Servs., Inc. MCI Telecomms. Corp.*, 14 FCC Rcd. 21579, 21614 (1999). "The traditional preponderance standard must be applied unless the type of case and the sanctions or hardship imposed require a higher standard." *Bender*, 744 F.2d at 1429. Given the hardship designation imposes on Huawei, the Commission should be required to meet this higher standard of proof. *See, e.g., Sea Island Broad. Corp.*, 627 F.2d at 244 (holding that the FCC was required to apply a "clear and convincing" standard when license revocation was tantamount to "a loss of livelihood"). In any event, as discussed below, the Commission fails to satisfy even the lesser "preponderance of the evidence" standard.

evidence that is "sufficiently reliable and probative to demonstrate that it is more likely than not that" a particular designation is proper. *See In re Universal Serv. Contribution Methodology*, 29 FCC Rcd. at 9720; *Consolidated Edison Co.* v. *NLRB*, 305 U.S. 197, 230 (1938); 5 U.S.C. § 556(d). Consequently, the Commission was not entitled to rely on materials that either do not constitute evidence or, even if they may be evidentiary in some sense, otherwise lack crucial indicia of reliability. Reliance on nonevidence or unreliable evidence to support a decision is arbitrary and capricious—and therefore unlawful. *Safe Extensions, Inc.* v. *FAA*, 509 F.3d 593, 604 (D.C. Cir. 2007). As explained below, nonevidence includes mere assertions, speculation, and arguments, *see infra* pp. 56-57; statutes, *see infra* pp. 57-58; and documents relying on indictments, *see infra* pp. 72-73. Impermissibly unreliable evidence includes congressional reports and other records of congressional proceedings, *see infra* pp. 59-62; hearsay lacking indicia of reliability, *see infra* pp. 74-75; and expert reports largely unreviewed by the Commission, *see infra* pp. 77-81. The Commission was not permitted to rely on any of these materials.[5]

In addition, the Commission was not permitted to rely critically on classified information. *See infra* pp. 81-82. Although the "Commission is authorized to withhold publication of records or proceedings containing secret information affecting the national defense," 47 U.S.C. § 154(j),

[5] The Commission relied on a series of fundamentally flawed "expert reports"—such as the Clarke Report, the Finite State Report, the Recorded Future Report, the RWR Report, and the 2009 DoD Annual Report—for its unsupported or mistaken conclusions about Chinese law; Huawei's ties to the Chinese government, military, and Communist Party; the security vulnerabilities of Huawei's equipment; and Huawei's governance and ownership structure. *See supra* pp. 79-81, 148-49. Moreover, the Commission doubly compounded its error by relying on the HPSCI Report, which itself relied on flawed expert reports—such as the NIST Interagency Report, the 2007 Defense Science Board Report, and the RAND Report—for its various conclusory and unreliable assertions on about Huawei's governance and ownership structure and ties to the Chinese government, military, and Communist Party; and its vague conclusion that Huawei seeks to control the telecommunications market. *See supra* pp. 69, 76-77. As explained above, the Commission also exaggerated the UK ISC, UK HCSEC, and 2019 NATO Report's conclusions about the identifiable security vulnerabilities in Huawei's equipment. *See supra* pp. 88-89.

the classified material cannot play a critical role in the agency's decision without appropriate due process safeguards. Courts have approved agency reliance on classified information only where "the unclassified material provided to [the affected party] is sufficient to justify the [decision]." *People's Mojahedin Org.* v. *U.S. Dep't of State*, 613 F.3d 220, 231 (D.C. Cir. 2010) (per curiam); *id.* (acknowledging that its cases have not decided whether "relying critically on undisclosed classified material would comport with due process"); *see also Fares* v. *Smith*, 249 F. Supp. 3d 115, 123 (D.D.C. 2017) ("[T]he D.C. Circuit [has] suggested a limit to the ability of the government to rely on undisclosed, classified information … [where] the classified record [is] essential to uphold [the] designation"). And even then, the government may be required to disclose the classified information "*ex parte* and *in camera*" to a neutral adjudicator. *Holy Land Found. for Relief & Devel.* v. *Ashcroft*, 333 F.3d 156, 164 (D.C. Cir. 2003) (discussing designations in the International Emergency Economic Powers Act context and noting that the statute authorizes *in camera* review of classified information for any decision that was based on classified information); *People's Mojahedin Org.*, 613 F.3d at 227 (noting that a court evaluates classified information).

The limitation on use of undisclosed, classified information is rooted in due process and administrative law principles. Due process requires that regulated parties against whom classified information is used in a critical way be given a meaningful opportunity to respond. *See, e.g.*, *Al Haramain Islamic Found., Inc.* v. *U.S. Dep't of Treasury*, 686 F.3d 965, 1001 (9th Cir. 2012) (concluding that an agency violated due process rights by "failing to provide constitutionally adequate notice and a meaningful opportunity to respond, and by failing to mitigate the use of classified information by, for example, preparing and disclosing an unclassified summary"); *KindHearts for Charitable Humanitarian Dev., Inc.* v. *Geithner*, 710 F. Supp. 2d 637, 660 (N.D. Ohio 2010) (suggesting that an agency would need to provide documents for *in camera* review by the affected

party's counsel if it could not declassify adequate information to provide constitutionally adequate notice). And, more generally, the APA and judicial review require a "full administrative record" to prevent an agency from "withhold[ing] evidence unfavorable to its case." *Walter O. Boswell Mem'l Hosp.* v. *Heckler*, 749 F.2d 788, 792 (D.C. Cir. 1984).

2. The evidence before the Commission showed that Huawei is a responsible provider of reliable and secure telecommunications equipment and services and that Huawei does not present a threat to national security

Huawei provided extensive comments and detailed exhibits during the rulemaking. That evidence overwhelmingly shows that: (a) Huawei is independent from the Chinese government; (b) Huawei adheres to leading cybersecurity practices; (c) Huawei's products have been subjected to rigorous testing by multiple oversight entities to ensure their integrity; and (d) Huawei's customers (both civilian and government) have expressed satisfaction with the safety of its products.

The Commission was obligated to consider Huawei's submissions on these points. More specifically, it was obligated to consider the whole record and "take into account whatever in the record fairly detracts from" the agency's conclusion, *Universal Camera Corp.*, 340 U.S. at 488, including "contradictory evidence or evidence from which conflicting inferences could be drawn," *Lakeland Bus Lines, Inc.* v. *NLRB*, 347 F.3d 955, 962 (D.C. Cir. 2003) (quoting *Universal Camera Corp.*, 340 U.S. at 487). That is because the Commission "cannot ignore evidence contradicting its position." *Butte County*, 613 F.3d at 194. And when the Commission relies on evidence, that evidence must be relevant to, and probative of, the point in question. *See supra* pp. 38-39. "An agency's refusal to consider evidence bearing on the issue before it constitutes arbitrary agency action." *Butte County*, 613 F.3d at 194. And "[t]he substantiality of evidence must take into account whatever in the record fairly detracts from its weight." *AT&T Corp.*, 86 F.3d at 247 (quotation marks omitted).

But the Commission flouted those standards. Huawei submitted thousands of pages of comments and evidence during the rulemaking proceeding. But while the Commission did indicate that Huawei "vigorously responded" to allegations that it posed a national security risk, it failed to meaningfully engage with that evidence, contenting itself with merely listing Huawei's submissions in a footnote without discussion. Order ¶ 43 n.123. That is insufficient. The Commission "must explain the evidence which is available," *State Farm*, 463 U.S. at 52, and "[t]o refuse to evaluate that information … is totally irrational," *Butte County*, 613 F.3d at 195. And because the Commission provided no notice to Huawei that it was the subject of an adjudication, it did not have the opportunity to supplement the record with that in mind. But even with that limitation, the affirmative evidence that Huawei submitted in the record during the rulemaking is by itself more than sufficient to demonstrate that the Commission's initial designation of Huawei was contrary to the weight of evidence in the record before it.

a. Huawei is independent from the Chinese government and will not acquiesce to Chinese government demands to engage in malicious cyberactivity

Huawei submitted hundreds of pages of comments and evidence demonstrating that it is independent of the Chinese government and is committed to cybersecurity.[6] The Commission did not meaningfully respond to this evidence or rationally explain why it could disregard it.

[6] Suffolk Decl. at 8-10; 6/1/2018 Purdy Decl.; 6/1/2018 Dowding Decl.; Ye Decl.; 6/1/2018 Chen & Fang Decl. ¶ 14; 2016 Huawei Cyber Security White Paper; 2014 Huawei Cyber Security White Paper 2014; 2013 Huawei Cyber Security White Paper; 2012 Huawei Cyber Security White Paper; Certification and Testing of Huawei Products; 7/2/2018 Purdy Supp. Decl. ¶¶ 20-25; 7/2/2018 Reply Decl. Dowding ¶¶ 7-13; deLisle Report at 7-10; 8/6/2018 Chen & Fang Supp. Decl.; 5/10/2019 Zhou Report at 16; 11/1/2019 Zhou Supp. Report ¶¶ 1, 3; Chen Rebuttal to Clarke Memo.

i. Huawei is a private company that is not controlled by the Chinese government.

As Huawei demonstrated through its comments and submissions during the rulemaking proceeding, Huawei is separate from and not beholden to the Chinese government.

First, Huawei USA is a subsidiary of Huawei Technologies, and both companies are wholly owned subsidiaries of Huawei Investment & Holding Co., Ltd. ("Huawei Holding"). Huawei Holding is a private company owned entirely by its employees (through an employee stock ownership plan) and by its founder, Mr. Ren Zhengfei. 6/1/2018 Dowding Decl. ¶ 10. The state holds no shares. deLisle Report at 4.

Second, as described above, Huawei is governed by a Board of Directors comprising 17 private citizens. 6/1/2018 Dowding Decl. ¶ 16. The company's business and investment decisions, research and development priorities, profit distributions, and staffing decisions are made and determined by the Board and are not controlled or influenced by the Chinese government, the Chinese military, or the Communist Party ("CCP"). *Id.* ¶¶ 14-17; 8/6/2018 Huawei Ex Parte at 41-42.[7] The Commission asserts that "the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions." Order ¶ 50. But as Huawei's experts have explained, Communist Party committees in private companies—required in all companies operating in China, including foreign-owned companies—do not and cannot exert that type of influence. *See* deLisle Report at 6-8, 17-19; Ye Decl. ¶¶ 29-30. "[T]here is a great deal of diversity and complexity in the relationships between the party or the state, on one hand, and business enterprises, on the other." deLisle Report at 2.

[7] Huawei now submits additional evidence confirming its independence from the Chinese government. *See* Ex. F, Expert Report of Randall Peerenboom ("Peerenboom Report"); Ex. C, Declaration of Alan Fanzhiyong ("Fanzhiyong Decl."); Ex. E, Declaration of Leon Wang ("Wang Decl."); Ex. F, Declaration of Huawei executive Wei Jiang ("Jiang Decl."); Ex. H, Expert Report of outside expert Dr. W. Jiang ("Jiang Report").

Huawei's ownership structure stands in stark contrast to state-owned companies or joint ventures like Nokia Shanghai Bell, whose key executives—including the chairman—are appointed by the Communist Party Organization Department. 8/6/2018 Huawei Ex Parte at 41 (citing Ex. 3-J, WTO Report WT-GC-W-745 (submitted as Ex. J to 8/6/2018 Huawei Ex Parte) ("WTO Report") and Ex. 3-K, "State-owned Enterprise Staffing Adjustment" (submitted as Ex. K to 8/6/2018 Huawei Ex Parte)). Unlike Huawei and other private enterprises, state-owned enterprises are pressured "to ensure that important company decisions are made in consultation with the enterprise's Party committee." WTO Report ¶ 1.10.

ii. Huawei executives attest to Huawei's independence from the Chinese government. Huawei understands that, "[a]s a global company headquartered in China," "it needs to be committed to going the extra mile in cyber security assurance." 2012 Huawei Cyber Security White Paper at 12. Accordingly, "Huawei does not, and would not, support, condone or conduct activities intended to acquire sensitive information related to any country, company or individual, nor [would it] knowingly allow [its] technology to be used for illegal purposes." *Id.* Huawei's Senior Corporate Vice President, Mr. Ding, testified before the HPSCI that Huawei "respect[s] all laws and regulations in jurisdictions where we operate" and "h[as] never, ever received a request [to inspect Huawei's communications equipment] from the Chinese government." Hearing on National Security Threats Posed by Chinese Telecom Companies Working in the U.S. Before the H. (Select) Intelligence Committee, 112th Con. 26 (2012) ("HPSCI Hearing"). And Huawei's founder, Ren Zhengfei has publicly stated on multiple occasions that, in any event, Huawei would refuse any request from the Chinese government to access the company's customer data. *See, e.g.*,

5/10/2019 Huawei Ex Parte at 4. Further, the record before the Commission contained two declarations from Huawei cybersecurity executives attesting to Huawei's independence from the Chinese government.

First, the record contains a declaration from John Suffolk, Huawei's Global Cyber Security and Privacy Officer, who was previously Her Majesty's Government Chief Information Officer and Senior Information Risk Owner for the United Kingdom Government. Suffolk Decl. at 1. Mr. Suffolk reports directly to Huawei's founder, has "had full and unfettered access to all Huawei people, facilities, documentation etc.," and has "full veto rights to block any product or solution if [he is] not satisfied with the security quality of the product." *Id.* at 6, 9. As Mr. Suffolk explained, he has "never been unduly influenced by any person within Huawei, or outside of Huawei, to reduce, stop, or alter any requirement [he] might have had that would, in [his] view, improve security by design, development or deployment—or indeed do anything that would weaken the safety and security of the products and services [Huawei] produce[s]." *Id.* at 6.

Second, Huawei submitted a declaration from Donald A. Purdy, Jr., Huawei's Chief Security Officer, who works with Suffolk and previously served as the senior cybersecurity official at the Department of Homeland Security from 2004 to 2006. 6/1/2018 Purdy Decl. ¶¶ 7, 9. Mr. Purdy further confirms:

> [D]uring [his] time at Huawei, [Mr. Purdy has] never learned any facts, nor [has he] received, or learned of, any allegations or been informed of allegations or even suspicions, that any employee, contractor, supplier, or partner of Huawei cooperated inappropriately with any government or any other organization or individual, to allow Huawei products (or third-party components) to be used for the unauthorized insertion of code (including for improper purposes, such as malicious code, programmable software, or code with an exploitable vulnerability) or, for malicious purpose, to intentionally allow a known, exploitable vulnerability to remain in code after discovery.

Id. ¶ 44. Mr. Purdy also does not know of any improper relationship between Huawei and the Chinese government. *Id.* ¶ 45. Lastly, as explained, Mr. Ren has stated that even if the Chinese government were to ask Huawei to engage in cyberespionage, Huawei would never do so. 5/10/2019 Huawei Ex Parte at 4.

b. Huawei adheres to leading cybersecurity practices

The comments and evidence that Huawei submitted to the Commission show that Huawei is an industry leader in the development and application of robust cybersecurity standards and policies.[8] The Commission did not meaningfully respond to this evidence or rationally explain why it could disregard it.

As Huawei explained, Huawei has "an end-to-end global cybersecurity system through stringent security policies and processes in every facet of its global operations that reflect international standards and guidelines, local laws and regulations, and feedback from vendors, employees, suppliers, and customers [with] enterprise-wide governance of cybersecurity and privacy policies and procedures." 6/1/2018 Huawei Comments at 6-9; *see also* 6/1/2018 Purdy Decl. ¶¶ 10-18. Huawei has undertaken a number of cybersecurity initiatives and is at the leading edge of risk assessment and management. *See, e.g.*, 2016 Huawei Cyber Security White Paper; 2014 Huawei Cyber Security White Paper 2014; 2013 Huawei Cyber Security White Paper; 2012 Huawei Cyber Security White Paper; *see also* Certification and Testing of Huawei Products (providing examples of Huawei's security, quality, and risk management certifications).

[8] 6/1/2018 Huawei Comments at 6-9; 6/1/2018 Purdy Decl. ¶ 10-32; Suffolk Decl. at 6, 16; 7/2/2018 Purdy Reply Decl. ¶¶ 22; 7/2/2018 Dowding Reply Decl. ¶ 6-14; 2012 Huawei Cyber Security White Paper; 2013 Huawei Cyber Security White Paper; 2014 Huawei Cyber Security White Paper; 2016 Huawei Cyber Security White Paper; Certification and Testing of Huawei's Products; 7/2/2018 Huawei Reply Comments at 61-64; 8/23/2018 Huawei Ex Parte; 3/12/2019 Huawei Ex Parte; 10/31/2019 Huawei Ex Parte; Niemi Report.

Huawei recognizes the "upstream" and "downstream" risks associated with "maliciously tainted products and counterfeit products" that are "all too often … not addressed" within the telecommunications industry. 2016 Huawei Cyber Security White Paper at 10-11; *see also, e.g.*, 2012 Huawei Cyber Security White Paper at 7 (identifying the potential threat of "[g]overnment-sponsored agents who use technology as they use other intelligence methods: to gather data and information on items of interest to them"); Suffolk Decl. at 4-5. Accordingly, "[a]s part of the effort to address supply chain risk, Huawei has established a comprehensive, ISO 28000-compliant supplier management system that can identify and control security risks during the end-to-end process from incoming materials to custom delivery." 2016 Huawei Cyber Security White Paper at 21; *see also id.* at 7 (identifying Huawei's "key success factors for addressing organizational security risk" as "commitment; governance; clear security requirements; consistent processes; performance metrics for individuals; internal compliance; and transparency"). In fact, Huawei remains the only 5G vendor in the industry to "require[] all of its technology vendors to sign cyber security agreements, and [to] work … to improve the security of [its] supply chain." Suffolk Decl. at 9 (noting that Huawei's "work with third-parties is rigorous, comprehensive and auditable").

Huawei follows the ABC model—"Assume nothing, Believe no one, and Check everything." 2014 Huawei Cyber Security White Paper at 12. And so it conducts laboratory testing that is "independent from R&D teams," *id.* at 14, by "third parties [that] must have the ability to re-test products and re-test changes to products after those changes or other fixes have been made," *id.* at 15. Huawei "encourage[s] audits, reviews and inspections on all technology vendors, including Huawei, in a fair and non-discriminatory manner, as every audit or review enables companies to challenge their thinking, policies and procedures, in turn enhancing their capability, product quality and product security." 2013 Huawei Cyber Security White Paper at 25.

Since 2011, Huawei has implemented "a transparent global assurance program … for cybersecurity and privacy." 6/1/2018 Purdy Decl. ¶ 10. Under this program, Huawei incorporates a Global Cybersecurity and Privacy Protection Committee that governs "enterprise-wide … cybersecurity and privacy policies and procedures" to which all Huawei employees must conform. *Id.* ¶¶ 10-18. Huawei also deploys a "robust supply chain assurance process of vetting and monitoring suppliers to ensure that suppliers are compliant with Huawei cybersecurity and privacy requirements." *Id.* ¶ 14. Further, Huawei has a dedicated team that conducts "periodic, unannounced audits of regional and national cybersecurity and privacy programs." *Id.* ¶ 17.

Specific to domestic operations, Huawei USA is also subject to "unannounced, periodic cybersecurity and privacy audits" led by an independent Cybersecurity and Privacy Committee chaired by its Chief Security Officer and with members appointed by Huawei USA executives. *See id.* ¶¶ 19-23. Huawei USA implements a "Services Cybersecurity Policy" that provides formal rules and processes for restricting access to customer networks. *See id.* ¶¶ 28-32. Huawei USA's has only limited access to customer networks for specific purposes that is subject to customer consent, control, and audit through mandatory use the Secure Network Access Solution ("SNAS"), which is isolated from Huawei's intranet and allows access to customer networks only by approved U.S.-based personnel, and the company maintains an independent and auditable U.S.-based Technical Assistance Center for remote support of these networks. *See id.* ¶¶ 24-27, 32; 7/2/2018 Dowding Reply Decl. ¶ 8 ("Huawei Technologies USA does not manage networks or provide services that involve storing the end user data of its carrier and enterprise customers in a manner that would give [it] access to its customers' network information."); 6/1/2018 Dowding Decl. ¶¶ 22, 24. Indeed, Huawei is "a champion of best practices, a champion of openness and transparency and a

champion of protecting user data" that "will never put the commercial interests of [the] company ahead of security." Suffolk Decl. at 11.

c. Huawei's products have been subjected to rigorous testing by multiple oversight entities to ensure their integrity

The evidence before the Commission also showed that Huawei's products have been subjected to rigorous testing by reliable and credentialed evaluators to ensure their integrity and protection against cybersecurity breaches. For example, the United Kingdom has worked with Huawei to establish the Huawei Cyber Security Evaluation Center ("HCSEC"), which is monitored by a public-private Oversight Board that ensures its independence. *See* 8/23/2018 Huawei Ex Parte at 1. The HCSEC is financed by Huawei and staffed by about forty individuals with security clearances who evaluate the security of Huawei products used in the UK. *See id.* For several years in a row, the Oversight Board has released reports concluding that the HCSEC provides high-quality technical assessments and cybersecurity expertise, and is effective at addressing any issues. *See id.* at 2-4. As Ciaran Martin, the head of the UK's National Cyber Security Centre, has stated, the UK's regime "is arguably the toughest and most rigorous oversight regime in the world for Huawei." 3/12/2019 Huawei Ex Parte at 3. But "the HCSEC, like other security certification bodies, has never found any malicious code or backdoor in Huawei's products." 8/23/2018 Huawei Ex Parte at 4; *see also* 7/2/2018 Huawei Reply Comments at 61-62 (compiling statements by Viaero Wireless, United Telephone Association, Inc., Mark Twain Communications Company, Pine Belt Cellular, and Sagebrush Cellular, Inc., regarding their purchase of Huawei's equipment and services without any cybersecurity incidents). As Huawei explained, and as expressly acknowledged by the head of the UK National Cyber Security Centre, any security problems "are not indicators of hostile activity by China." 3/12/2019 Huawei Ex Parte at 3 (quoting Ciaran Martin, Head of UK National Cyber Security Centre). Further, a recent article written by the former

minister of the UK's Department of Digital Culture, Media, and Sport confirms that problems identified in Huawei's products and engineering "have been comparable to the sorts of issues that might arise from this level of scrutiny of any companies' products, and are not consistent with a serious threat to [the UK's] national security." Ex. AA, Margot James, *The Evidence Available Does Not Support a Total Ban on Huawei*, Conservative Home (Jan. 24, 2020).[9]

As Huawei has shown, products of Huawei USA are also "subject to third-party testing" and "internal and external processes that can detect and protect against possible malicious acts by third parties or insiders; for example, the plant of a backdoor or other hidden functionality not covered in the product manual, or vulnerability, or allowing significant, known vulnerabilities to remain unpatched." 6/1/2018 Purdy Decl. ¶ 24. Huawei has "two independent labs, not under Huawei control, one in the UK and one in Canada that independently assure [its] products." Suffolk Decl. at 9. Additionally, "customers are free to adopt any verification method they wish, [as] a wide range of security testing companies from the USA, Europe and Asia … validate [its] products." *Id.*

For more than five years, EWA North America has served as an independent laboratory performing security evaluations for vendors, such as Huawei USA, and "Trusted Delivery" verifications for network carriers. *See* 6/1/2018 Purdy Decl. ¶ 34. EWA's testing personnel are thoroughly vetted and possess high-level government security clearances. *See id.* ¶ 35. Due to risks

[9] The Commission cited a pair of reports from the security community in the United Kingdom that it said "sounded the alarm about the risks associated with Huawei's engineering process," but neither supports designation, and the Commission's claim is contrary to the reports' own conclusions and the evidence Huawei submitted. Order ¶ 55 & nn.170-72 (citing UK Huawei Cyber Security Evaluation Centre, *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report* (2019) ("2019 HCSEC Report") and UK Parliament Intelligence and Security Committee, *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security* (June 2013) ("UK ISC Report")).

associated with vendors that work with state actors, EWA's testers do not provide vendors with any insight into test protocols or the standards being applied. *See id.* ¶¶ 36-37; 2013 Huawei Cyber Security White Paper at 26-27. After testing, EWA deploys *all* software directly to supported carriers via "Trusted Delivery" so that the carriers get exactly what was tested—not alternative versions that could have been modified. *See* 6/1/2018 Purdy Decl. ¶¶ 38-39 ("EWA NA conducts in-depth testing of a statistically significant sample of assemblies that are chosen at random by the Carrier organization. All software releases, patches and hardware upgrades throughout the lifecycle of the deployment, [a]re fully evaluated by EWA NA prior to deployment."); *see also* Suffolk Decl. at 9-10 (noting that Huawei uses "secure international shipping companies"). This process "has long been validated by both carrier and key government experts as a valid solution to a wide array of threat/risk concerns," because it allows "a customer [to] maintain full surveillance of all aspects of the systems and software design designated for deployment, and it provides high-fidelity protection against the malicious introduction of unevaluated technology." 6/1/2018 Purdy Decl. ¶ 40.

As with its treatment of evidence regarding Huawei's leadership in developing cybersecurity standards, the Commission largely ignored the comments and evidence Huawei submitted and discussed above regarding the security of Huawei's products. Although the Commission cited purported expert reports pertaining to product integrity without addressing Huawei's submissions (Order ¶¶ 54-57), as discussed *supra* pp. 77-81, the assertions made in those reports lack reliability and are flawed in multiple ways involving, for instance, the testing of wrong equipment.

d. Huawei's customers (both civilian and government) have expressed satisfaction with the safety of its products

The evidence before the Commission also demonstrated that, Huawei's international reputation for customer satisfaction is strong, in no small part because of Huawei's commitment to

cybersecurity and product innovation. In fact, by the end of 2017, 197 Fortune Global 500 companies—45 of which are Fortune 100 companies—had chosen Huawei's network technology offerings for their digital transformation.[10] *See* Ex. 5-A, 8/27/2018 Huawei FTC Comments at 26 (citing Huawei Investment & Holding Co., Ltd. 2017 Annual Report). Huawei equipment is widely used in over 170 countries across the world today without undermining any nation's security. *See* 6/1/2018 Huawei Comments at 86-87; 6/1/2018 Dowding Decl. ¶ 7. And there is no evidence—in the record or otherwise—that equipment manufactured or sold by Huawei has produced a national security risk. *See id.*; *see also supra* pp. 49-51 (discussing Huawei's cooperation with the UK through HCSEC, which has never found any malicious code or backdoor in Huawei's products).

To the contrary, the governments and public entities of many countries, such as the UK, Canada, and Finland have expressed confidence or continue to demonstrate trust in Huawei's equipment. *See* 7/2/2018 Huawei Reply Comments at 62-63; *infra* pp. 149-56 (discussing foreign governments maintaining their relationship with Huawei). For example, a spokesman for the UK's National Cyber Security Centre explained that the British "government and [] telecoms operators work with Huawei at home and abroad to ensure the UK can continue to benefit from new technology while managing cyber security risks." *Id.* Likewise, in Canada, Bruce Rodin, an executive who manages the wireless networks for Bell Canada and uses cyber-security firms to extensively test Huawei's products, stated that his company has "never seen malicious code or backdoors." *Id.*

[10] Huawei now submits additional evidence showing that the number of companies using Huawei equipment has only increased. By the end of 2018, 211 Fortune Global 500 companies—48 of which are Fortune 100 companies—had selected Huawei as their partner for digital transformation. 2018 Huawei Annual Report at 27.

As a result, many countries in Europe, Africa, the Middle East, and the Americas plan for further deployment of Huawei's 5G equipment. *See* 11/12/2019 Huawei Ex Parte at 2. The Commission identifies a few countries—New Zealand, Japan, and Australia—that have chosen to exclude Huawei from their rollout of 5G networks. *See* Order ¶ 53. But the Commission ignores the numerous other countries, including close allies such as the UK, that plan to incorporate Huawei equipment in the deployment of their 5G infrastructures. *See, e.g.*, 3/12/2019 Huawei Ex Parte at 3-4 (identifying the extensive security collaborations between the United Kingdom and Huawei, and clarifying that New Zealand has not yet decided to ban Huawei from its 5G network); 6/12/2019 Huawei Ex Parte at 6-8 (explaining that Germany, France, and Canada have opted not to ban Huawei from their telecommunications infrastructures); 11/12/2019 Huawei Ex Parte at 2-5 (adding Hungary and Norway to the list of countries declining to ban Huawei from their 5G networks; identifying Greece's partnership with Huawei for two 5G pilot networks and Portugal's partnership with Huawei for its first 5G mobile city); *see also* 6/12/2019 Huawei Ex Parte at 4-7 (collecting quotations from domestic and international cybersecurity officials acknowledging that the complexity and inherent risks of the global supply chain counsel for risk-based assessments rather than company-specific bans).

Huawei submitted ample evidence pertaining to other countries' use of Huawei products, and that evidence further demonstrates the products' reliability and security. In response, the Commission claimed that it would look to "allies for their assessment of the risk posed by Huawei, but not for specific policy guidance on how to respond to this threat." Order ¶ 53 n.160. But the Commission merely cited articles reporting other countries' exclusionary policy decisions. The Commission did not explain what objective risk assessments it thought those other countries had made, and whether or how it was relying on those underlying assessments. Instead, the Commission

pointed merely to what those countries have purportedly chosen to do as a policy matter—*i.e.*, the very thing the Commission said it was not doing. And the articles the Commission cited undermine the claim that those countries conducted any objective risk assessments. Those articles expressly acknowledged the United States' role in pressuring those countries to exclude Huawei. Order ¶ 53 nn.163-65. That U.S. pressure, of course, was based on politically expedient prejudgment; thus, to the extent other countries bowed to it, they simply compounded the problem. *See infra* pp. 59-71, 114-24. The Commission cannot launder the prejudgment through backdoor diplomacy. Moreover, to the extent other countries performed security risk analyses, the Commission cherry-picked the countries with negative assessments, while ignoring other countries' positive assessments. The Commission's failure to "take into account whatever in the record fairly detracts" from the reasons for its designation, once again, rendered the designation invalid. *AT&T Corp.*, 86 F.3d at 247.

e. Huawei's presence would improve, not threaten, competition and diversity

Additionally, the Commission irrationally failed to consider how banning Huawei from the marketplace will delay domestic 5G deployment, thereby adversely impacting GDP and causing the loss of tens of thousands of jobs. *See, e.g.*, Aron Report I ¶¶ 174-94. The Commission erroneously averred that because "[t]he four largest U.S. mobile carriers do not use and have no plans to use Huawei … radio access network equipment," its designation of Huawei will not delay U.S. 5G deployment or increase 5G equipment prices, and instead will enable "continued U.S. leadership in 5G." Order ¶ 121.

Indeed, the lack of competition generated by Huawei's market presence will substantially drive up prices, reduce coverage, degrade customer support, and introduce uncertainty—to the particular detriment of rural carriers. *See* Aron Report I ¶¶ 195-218; Ex. 22, 6/1/2018 CCA Comments at 7-13; *e.g.*, 22-A, Declaration of Steven K. Berry at 1-6 (submitted as Ex. A to 6/1/2018

CCA Comments) ("Berry Decl.") ("Rural carriers must contend with higher costs and larger and more sparsely populated geographic coverage areas" and that, for low-volume purchasers, Huawei and ZTE's equipment is "often two or three times less expensive" than their competitors.); Ex. 22-B, 6/1/2018 CCA Declaration of Michael Beehn at 1-3 (submitted as Ex. B to 6/1/2018 CCA Comments) ("Beehn Decl.") (representing SI Wireless, LLC and its 20,000 customers in Kentucky and Tennessee, and noting that the Commission's rule will make it "very difficult, if not impossible, for SI Wireless to maintain its current network and implement future network upgrades"); Ex. 22-C, Declaration of Frank DiRico at 1-3 (submitted as Ex. C to 6/1/2018 CCA Comments) ("DiRico Decl.") (representing Viaero Wireless and its 110,000 customers in Colorado, Kansas, Nebraska, Wyoming, and South Dakota, and explaining that the Commission's rule will result in significant outages and replacement and interoperability costs of over $400 million); Ex. 22-D, Declaration of James Groft at 1-3 (submitted as Ex. D to 6/1/2018 CCA Comments) ("Groft Decl.") (representing James Valley Telecommunications and its 10,000 customers in South Dakota, and explaining that Huawei's equipment is the "most cost-effective option with a 40% savings versus the 2nd most cost-effective option"); Ex. 22-E, Declaration of Todd Houseman at 1-2 (submitted as Ex. E to 6/1/2018 CCA Comments) ("Houseman Decl.") (representing United Telephone Association, Inc. and its 20,000 customers in Kansas, and noting that Huawei's equipment is their most cost-effective option); Ex. 22-F, Declaration of Michael D. Kilgore at 1-2 (submitted as Ex. F to 6/1/2018 CCA Comments) ("Kilgore Decl.") (representing Nemont Telephone Cooperative, Inc. and its 12,000 customers in Montana and North Dakota, and asserting that the Commission's rule "threatens to put Nemont out of the wireless business and leave its customers without wireless service"); Ex. 22-H, Declaration of Eric J. Woody at 1-4 (submitted as Ex. H to 6/1/2018 CCA Comments) ("Woody Decl.") (representing Union Telephone Company and its

40,000 customers in Wyoming, Colorado, Utah, and Idaho, and stating that the Commission's rule threatens to cause network outages and loss of emergency services, halt "critical projects," and put "Union's ability to survive … into serious question").

3. The Commission's decision to designate Huawei, despite Huawei's ample affirmative evidence, improperly rested on nonevidence and unreliable evidence

The Commission bore the burden of proving by a preponderance of the evidence that designation of Huawei was warranted. But the Commission's initial designation of Huawei is unsupported by reliable evidence—and, in most respects, is unsupported by any evidence at all. Instead, the Commission relied on materials that either do not constitute evidence, or, if they are evidence, are of the most unreliable sort: statutes, indictments, hearsay lacking indicia of reliability, "expert" reports that lack supporting documentation and have not been independently reviewed by the Commission, and undisclosed classified information that Huawei had no opportunity to address.

Indeed, the Commission's Order is riddled with improper reliance on speculation, assertion, and argument. But ipse dixit is not proof. When an agency's declaration of fact is unsupported by record evidence but is "capable of exact proof," the agency's asserted "fact" must be disregarded as arbitrary. *McDonnell Douglas Corp.* v. *Dep't of the Air Force*, 375 F.3d 1182, 1190 n.4 (D.C. Cir. 2004); *see also Safe Extensions*, 509 F.3d at 604-05 (noting the holding of *McDonnell Douglas Corp.* and finding the agency "provided absolutely no evidence to back … up" differential treatment of regulated parties); *Can. Commercial Corp.* v. *Dep't of the Air Force*, 442 F. Supp. 2d 15, 35 (D.D.C. 2006) (holding that an agency cannot simply articulate an "unsubstantiated rationale" which is "quite capable of substantiation"), *aff'd*, 514 F.3d 37 (D.C. Cir. 2008). And "[s]peculation is, of course, no substitute for evidence" in agency adjudications or elsewhere. *White ex rel. Smith* v. *Apfel*, 167 F.3d 369, 375 (7th Cir. 1999). Speculation, assertion, and arguments are therefore not evidence sufficient to establish a fact.

The Commission's reliance on nonevidence and fatally unreliable evidence, rather than reliable evidence, means that Huawei's designation will be unable to survive even deferential judicial review for substantial evidence. *Cf.* 5 U.S.C. § 556(d); *U.S. Steel Min. Co., Inc.* v. *Director, Office of Workers' Compensation Programs*, 187 F.3d 384, 388-89 (4th Cir. 1999) (identifying agencies' important "gate keeping function while assessing evidence," and requiring agencies to maintain "discipline to qualify evidence" in order to satisfy their burden of proof). And the designation certainly is unsupported by a *preponderance* of the evidence.

a. The Commission erroneously relied on statutes as evidence against Huawei

To begin, the Commission states that, to determine whether an entity is a national security risk under the rule, it will rely on, among other things, "determinations by … Congress or the President that an entity poses a national security threat." Order ¶ 41. Consistent with this statement, the Commission looked to the passage of the 2018 and 2019 NDAAs as the basis for establishing facts critical to its designation. *See* Order ¶¶ 12, 13, 45, 48.

That was impermissible. Courts have recognized in the context of judicial proceedings that "[s]tatutes are not evidence," *Porter* v. *Shineski*, 650 F. Supp. 2d 565, 568 (E.D. La. 2009), and the reasons behind this conclusion apply equally to agency adjudications. In particular, "[b]ecause legislatures are 'not obligated, when enacting [their] statutes, to make a record of the type that an administrative agency or court does to accommodate judicial review,' [one] should not conflate legislative findings with 'evidence' in the technical sense." *Pena* v. *Lindley*, 898 F.3d 969, 979 (9th Cir. 2018) (quoting *Minority Television Project, Inc.* v. *FCC*, 736 F.3d 1192, 1199 (9th Cir. 2013) (en banc)); *see also Minority Television Project*, 763 F.3d at 1199 ("Congress is a political body that operates through hearings, findings, and legislation; it is not a court of law bound by federal rules of evidence."). Relying on statutes in an adjudication raises constitutional due process

concerns as well, since any factual assertions contained therein would have remained uncorroborated and untested. *Pena*, 898 F.3d at 979; *Lothrop* v. *Stedman*, 42 Conn. 583, 926 (C.C.D. Conn. 1875) ("[A] legislature has no power to find facts by legislative enactment, so as to be evidence in suits against persons who were not applicants for the act"). Further, allowing congressional action, where there are no adjudicative protections, to serve as a irrefutable assertion in an adjudication would "erode" the "carefully defined limits on the power" of each branch of government. *INS* v. *Chadha*, 462 U.S. 919, 957-58 (1983) ("To preserve those checks, and maintain the separation of powers, the carefully defined limits on the power of each Branch must not be eroded.").

The statutes at issue here, the 2018 and 2019 NDAAs, restrict Huawei from selling its equipment or services to federal agencies, contractors, and loan and grant recipients. The Commission cited these statutes in support of its broad, unverified claims regarding Huawei's purported connections to the Chinese government. *See* Order ¶ 45 & n.132 (asserting "legislative concern" related to Huawei as "pos[ing] a great security risk because Chinese intelligence agencies have opportunities to tamper with their products in both the design and manufacturing processes"); *id.* ¶ 48 & n.142 (alleging Huawei's "long-term security risks and ... close ties to the Chinese government"). But because statutes are not evidence, the Commission may not rely on the NDAAs to make such factual findings. That is because any findings made during the legislative process are not subject to scrutiny in any impartial court or adjudicatory body, and congressional statements made during that same process are inadmissible as unreliable hearsay. Moreover, in imposing legal sanctions under the statutes, Congress made no express factual findings anyway. For all these reasons, the Commission cannot rely on the NDAAs to meet its burden.[11]

[11] What is more, the 2019 NDAA violates the Bill of Attainder Clause of the Constitution, and so cannot be relied on in any respect whatsoever. *See* Ex. SS, Pls.' Mot. for Summ. J. at 10-

b. The Commission erroneously relied on the HPSCI Report as evidence against Huawei

The Commission's reliance on the HPSCI Report was arbitrary and capricious. As explained below, the Commission was not permitted to rely on such unreliable congressional materials. And an examination of the report shows that it is highly prejudicial and unreliable.

i. The Commission was not permitted to rely on congressional reports and other records of congressional proceedings as reliable evidence. Courts have consistently doubted the evidentiary value of congressional proceedings and reports. Congressional proceedings lack the "substantive rules" and "procedural safeguards" applicable to courts. *Chadha*, 462 U.S. at 964-65 (Powell, J., concurring in the judgment). And the inherently political nature of congressional proceedings is "hardly conducive to the development of facts." *Knight Pub. Co.* v. *U.S. Dep't of Justice*, 631 F. Supp. 1175, 1178 (W.D.N.C. 1986). Consistent with these limitations, the Framers determined that Congress may not conduct adjudications, *see Chadha*, 462 U.S. at 964-65 (Powell, J., concurring in the judgment), because to allow Congress to "decide[] rights of specific persons" would be to subject those rights to "the tyranny of a shifting majority." *Id.* at 966. This same judgment underlies the Constitution's Bill of Attainder Clause, which equally recognizes that the legislature is not suited to make adjudicative judgments, and instead should be limited to making generally applicable rules. *See, e.g.*, *United States* v. *Brown*, 381 U.S. 437, 445-46 (1965). Because Congress is bound by neither "substantive rules" nor "procedural safeguards, such as the right to counsel and a hearing before an impartial tribunal, that are present when a court or an agency adjudicates individual rights," the "only effective constraint on Congress' power is political," and

28, *Huawei Techs. USA, Inc., et al.* v. *United States, et al.*, No. 4:19-cv-00159-ALM (E.D. Tex. filed Mar. 6, 2019).

"Congress is most accountable politically when it prescribes rules of general applicability." *Chadha*, 462 U.S. at 964-65 (Powell, J., concurring in the judgment).

Therefore, "[c]ourts have consistently excluded congressional reports" as evidence "because of the inherently political nature of the reports." *Richmond Med. Ctr.* v. *Hicks*, 301 F. Supp. 2d 499, 512 (E.D. Va. 2004), *rev'd on other grounds*, 570 F.3d 165 (4th Cir. 2009); *see also Baker* v. *Firestone Tire & Rubber Co.*, 793 F. 2d 1196, 1199 (11th Cir. 1986) (finding that a congressional report of an investigation into failed Firestone tires lacked trustworthiness and was thus inadmissible because it was politically motivated). Simply put, because Congress is a "politically-motivated" body, "[t]here would be too great a danger political considerations might affect the findings of" is committee reports. *Pearce* v. *E.F. Hutton Grp., Inc.*, 653 F. Supp. 810, 813-15 (D.D.C. 1987); *see also Barry* v. *Trs. of Int'l Ass'n Full-Time Salaried Officers & Emps. of Outside Local Unions & Dist. Counsel's (Iron Workers) Pension Plan*, 467 F. Supp. 2d 91, 97 (D.D.C. 2006) (weighing concern that "political considerations, as well as elected officials' tendency to 'grandstand,' have influenced the factual findings, conclusions, or opinions included in Congressional reports") (citations omitted).

The courts addressing this issue have drawn a sharp contrast between methodical, objective judicial and quasi-judicial proceedings, which generally carry sufficient indicia of trustworthiness, and the unconstrained and potentially politically charged proceedings in Congress, which do not. In *Baker*, for example, the Eleventh Circuit found that a congressional subcommittee report on an investigation into the company's tires "lack[ed] the trustworthiness necessary" because the "subcommittee report did not contain the factual findings necessary to an objective investigation, but consisted of rather heated conclusions of a politically motivated hearing." 793 F.2d at 1199; *see also Bright* v. *Firestone Tire & Rubber Co.*, 756 F.2d 19, 22-23 (6th Cir. 1984); *Anderson* v. *City*

of New York, 657 F. Supp. 1571, 1579 (S.D.N.Y. 1987) (contrasting congressional hearings, "so termed," and the kinds of hearings "held by administrative agencies in their quasi-judicial capacity"). Critically absent in many congressional proceedings is any assurance of an independent, thorough, and fair-minded investigation. In *Bright*, for example, the Sixth Circuit held that a congressional subcommittee report premised on lawsuits and consumer complaints lacked the requisite trustworthiness because the subcommittee did not investigate the grounds for any of those complaints. 756 F.2d at 22. The court pointed to "[t]he unverified nature of the evidence relied on by the Committee." *Id.* at 22-23; *see also, e.g.*, *United States* v. *Davis*, 826 F. Supp. 617, 623-24 (D.R.I. 1993) (documents that "merely report what was told to the investigators by witnesses, [without] draw[ing] inferences as to what in fact happened" and that are "pervaded by hearsay" are considered untrustworthy); *see also United States* v. *Taylor*, 462 F.3d 1023, 1026 (8th Cir. 2006) (finding police report was not admissible under the Federal Rules of Evidence where it "contained only a recitation of the citizen's statements to the police").

When assessing the admissibility of public records under Federal Rule of Evidence 803(8), courts have been guided by "a nonexclusive list of four factors which are helpful in determining trustworthiness: (1) the timeliness of the investigation; (2) the special skill or expertise of the official; (3) whether a hearing was held and at what level; and (4) possible motivational." *Moss* v. *Ole S. Real Estate, Inc.*, 933 F.2d 1300, 1305 (5th Cir. 1991). As detailed below, the HPSCI Report fails on most of those factors. Beyond merely those factors, the analysis depends "primarily [on] whether the report was compiled or prepared in a way that indicates that its conclusions can be relied upon," *id.* at 1307, an assessment that in turn "focuses on the methodology behind the report," *id.* at 1308 (citing *Broadcast Music, Inc. v. Xanthas, Inc.*, 855 F.2d 233, 238-39 (5th Cir.

1988)). A straightforward analysis of these factors makes clear that the HPSCI Report is unreliable and cannot provide any support for designation of Huawei.

ii. The Commission erroneously relied on the HPSCI Report. Throughout its Order, the Commission relied on the HPSCI Report to establish facts it deemed relevant to support its designation decision,[12] but the Commission's trust in the HPSCI Report is misplaced. Nothing in that report constitutes evidence to support a finding that can be relied on by the Commission for its designation because it lacks the necessary indicia of trustworthiness, which matter no less in the agency context than they do in judicial proceedings. *See supra* pp. 38-39.

Most fundamentally, the HPSCI Report lacks the requisite trustworthiness because (1) it was politically motivated; (2) it was inaccurate, incomplete, and relied largely on innuendo rather than actual facts; and (3) even if it purported to contain factual findings, its process was, as discussed in more detail below, rife with procedural and methodological flaws that completely undercut the HPSCI Report's reliability including, among other things, its reliance on certain, often undisclosed or confidential sources making unproven allegations containing multiple levels of

[12] For example, the Commission relied on the HPSCI Report to purportedly establish that: Huawei has a history "that includes connections to the Chinese government," Order ¶ 7; *see also* ¶ 45 (citing HPSCI Report at 3-4); Huawei's founder has ties to the People's Liberation Army ("PLA"), *id.* ¶ 50 (citing HPSCI Report at 13-14); Huawei once provided special network services to an entity believed to be an elite cyber-warfare unit within the PLA, *id.* ¶ 50 (citing HPSCI Report at 34); Chinese intelligence agencies could tamper with Huawei's products in both the design and manufacturing process, *id.* ¶¶ 45, 46 (citing HPSCI Report at 3-4); the Chinese government can exert influence over Huawei through the company's internal communist party committee, *id.* ¶ 50 (citing HPSCI Report at 23); the Chinese government can exert influence over Huawei generally, *id.* ¶ 49 n.147 (citing HPSCI Report at 11); and Huawei's low costs are due to favorable subsidies and benefits bestowed on them by China, *id.* ¶ 30 (citing HPSCI Report at 21, 27-31). The Commission also relied on the HPSCI Report to show that when companies "seek to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries," before boldly asserting with no citation that Huawei seeks to limit market diversity. Order ¶ 56 (quoting HPSCI Report at 2).

hearsay without any opportunity for cross-examination or response, borrowing uncritically from outside sources without independent evaluation, and reliance on incorrect notions of Chinese law.

First, the HPSCI Report emerged almost eight years ago from an inherently and pervasively political process, not an objective investigation of facts. As detailed below in the discussion of the HPSCI Report's sources, the report was produced without the procedural safeguards necessary to render its "findings" reliable. More fundamentally, the entire process was "marred by political expediency." *Anderson*, 657 F. Supp. at 1579. As one court has warned, "[g]iven the obviously political nature of Congress, it is questionable whether any report by a committee or subcommittee of that body could be admitted … against a private party. There would be too great a danger that political considerations might affect the findings of such a report." *Pearce*, 653 F. Supp. at 814. Just so here. The report was released in October 2012, just in time for its use in an important election year. 6/1/2018 Huawei Comments at 90; *see also, e.g.*, Ex. BB, Charles Arthur, *China's Huawei and ZTE Pose National Security Threat, says US Committee*, Guardian (Oct. 8, 2012) (The report "become fodder for a presidential campaign in which the candidates [had] been competing over their readiness to clamp down on Chinese trade violations."); Ex. CC, Jim Wolf, *U.S. Lawmakers Seek to Block China Huawei, ZTE U.S. Inroads*, Reuters (Oct. 7, 2012) (discussing the report and noting that "China has also been a frequent target on the campaign trail, with President Barack Obama and Republican challenger Mitt Romney both saying the United States needs to get tougher on China for alleged abusive trade practices"). "[T]he politics [were] palpable at a time when U.S. presidential candidates [were] busy sparring over China's trading practices and invoking the 'get tough' mantra. … [M]any in China will see the U.S. Congress as engaging in trade protectionism disguised as security policy." Ex. DD, Simon Montlake, *U.S. Congress*

Flags China's Huawei, ZTE as Security Threats, Forbes (Oct. 8, 2012). These circumstances created precisely the "politically motivated" process, *Baker*, 793 F.2d at 1199, rife with "political considerations, as well as elected officials' tendency to 'grandstand,'" *Barry*, 467 F. Supp. at 97, that have led courts to "consistently exclude[]" reports like the HPSCI Report for lacking the requisite indicia of reliability and trustworthiness to constitute probative evidence, *Richmond Med. Ctr.*, 301 F. Supp. 2d at 512. Indeed, media coverage at the time recognized that the report, "com[ing] at a time of rising trade friction, thanks to the election," lacked evidentiary support for its recommendations. Ex. EE, "Huawei and ZTE: Put on Hold," *The Economist* (Oct. 13, 2012) (noting that the report "appears to have been written for vegetarians. At least, there is not much meat in it.").

Second, the HPSCI Report does not actually make the factual findings that the Commission seemed to assume it does. For a congressional report to produce factual findings—even assuming an adjudicatory tribunal could later afford them any weight, *but see supra* pp. 59-62—it must be the product of an "investigation whose stated purpose was the resolution of some factual dispute." *Pearce*, 653 F. Supp. at 814. Here, the Committee did not make conclusive determinations based on evidence but instead, by its own terms, made tentative observations recommending further investigation. For instance, the report asserted vaguely that Huawei "*likely* remains dependent on the Chinese government for support," HPSCI Report at 13 (emphasis added); that Huawei "*may* have connections and ties to Chinese leadership," *id.* at 24; that the Committee "*considers it possible* that Huawei receives substantial support from the Chinese government," *id.* at 30; that the Committee's "concerns" are "*heighten[ed]* about Chinese government control over these firms and their operations," *id.* at 12; and that the Committee has "*serious doubts* about whether Huawei can be trusted to operate in the United States in accordance with United States legal requirements and

international codes of business conduct," *id.* at 13. (emphases added); *see id.* at 34-35. Indeed, even while faulting Huawei, the HPSCI Report also admitted that the Committee "did not attempt a review of all technological vulnerabilities of particular ZTE and Huawei products or components." *Id.* at vi-vii, 11. These vague, equivocal assertions and recommendations do not come close to providing the "resolution of [a] factual dispute" necessary to produce reliable factual findings, *Pearce*, 653 F. Supp. at 814, even assuming Congress has the power to make consequential factual findings—about a single entity or two, no less.

Moreover, the Committee based its conclusions on the supposed *absence* of evidence rather than on any actual proof of wrongdoing or misconduct. Despite Huawei's extensive submissions of documents and interviews, the Committee thought Huawei's failure to provide still greater detail on certain points "suspicious," HPSCI Report at 23, and declared even uncontroverted explanations "not credible," *id.* at 26; *see also id.* at 34. Indeed, fully ten of the HPSCI Report's twelve distinct "findings" rested in whole or part not on affirmative evidence gathered by the Committee but on perceived shortcomings in Huawei's efforts to allay the Committee's unsupported suspicions. *See id.* at 13-35. Even if these purported shortcomings were genuine, the Committee at one point acknowledged that they "do[] not prove wrongdoing." *Id.* at vi. The Committee's suspicions certainly cannot satisfy the Commission's burden here of providing affirmative evidence of wrongdoing.

Third, even if the HPSCI Report did contain such factual findings about Huawei's ties to China and the ability of the Chinese government to exert influence over Huawei, those findings would be untrustworthy and unreliable. *See Moss*, 933 F.2d at 1307-08. As explained in detail below, the report (a) relied throughout on sources that are not identified in the report and that make

unproven allegations containing multiple levels of hearsay; (b) borrowed uncritically from "expert" sources without independent evaluation as to their reliability and without any apparent analysis of the sources on which those analysts and reports relied; and (c) based its assertions on a false notion of Chinese law without analysis and expertise.

a. The HPSCI Report relied throughout on unidentified or confidential sources. A report that relies on non-public or otherwise undiscoverable sources and that is "pervaded by hearsay" presents grave trustworthiness problems. *Davis*, 826 F. Supp. at 623-24. And although anonymity may not automatically render a source unreliable, an accusation of wrongdoing must still "unambiguously provid[e] in a cognizable and detailed way the basis of the [anonymous source's] knowledge." *Mizzaro* v. *Home Depot, Inc.*, 544 F.3d 1230, 1239-40 (11th Cir. 2008) (collecting cases). The report here contained purported factual findings derived from unidentifiable sources lacking any detail regarding the basis of their supposed knowledge.

The Committee purported to interview "former Huawei employees" and "industry experts," but it did not disclose any of their names (save two) or the circumstances under which those interviews were conducted or whether any formal records were kept. *Id.* at 8-10. Nor did the Committee provide any information about whether Committee staff members administered oaths to those interviewees or otherwise implemented processes to ensure that the information they provided was reliable. *Cf. Chambers*, 410 U.S. at 298 (noting that hearsay statements are "traditionally excluded because they lack the conventional indicia of reliability; they are usually not made under oath or other circumstances that impress the speaker with the solemnity of his statements"). Further, no information was provided about whether staff conducting interviews had expertise to evaluate witnesses "especially regarding their credibility or accuracy of recall." *Anderson*, 657 F. Supp. at 1579. And of course, Huawei had no opportunity to cross-examine any of those witnesses.

The hearsay from these "former Huawei employees" purportedly accused Huawei of engaging in "potentially unethical or illegal behavior." HPSCI Report at 11, 34-35. Specifically, the report claimed that "several former and current Huawei employees" alleged that Huawei purportedly committed, among other things, "[i]mmigration violations," "[d]iscriminatory behavior," and "bribery." *Id.* at 34-35. But the report failed to identify a single employee who purportedly made such claims. *Id.* at 11 n.32. It also failed to offer any detail about the date, place, or substance regarding such claims to allow Huawei to respond to the substance of these claims. Nor is it clear how these unsubstantiated and conclusory accusations (wholly unrelated to national security) establish that Huawei is a risk to the telecommunications networks or supply chain.

The report claims, relying solely on information purportedly provided by a former employee, "that Huawei provides special network services to an entity [the] employee believes to be an elite cyber-warfare unit with the [People's Liberation Army]." HPSCI Report at 34. Huawei expressly denied this unverified claim in response to the Committee—a response that Huawei submitted under penalty[13] but that the Committee failed to acknowledge. Ex. K, 9/22/2012 Huawei Second Responses to HPSCI's Questions at 12 ("9/22/2012 Huawei Second Responses to HPSCI"). The Committee also failed to disclose the employee's identity or his position within the company, and the Committee further purported to rely on "internal Huawei documentation," which it said was "dated July 1, 2011" and "appear[ed] authentic" without explaining why it appeared so or disclosing the document for examination or corroboration. HPSCI Report at 34 n.131. And the Committee did not provide any information regarding what "entity" was supposedly serviced or what kind of "special network services" were purportedly provided. Such a vague and conclusory

[13] The penalty for making a false statement to Congress carriers serious consequences: A party who "makes or uses any false writing or document" "shall be fined … [or] imprisoned not more than 5 years." 18 U.S.C. § 1001(a).

accusation lacking sufficient detail about Huawei's purported ties to the Chinese military cannot justify the Commission's designation of Huawei.

The Committee also claimed to have relied on classified information, including in the report a "classified annex [that] provides significantly more information adding to the Committee's concerns." *Id.* at 10. But the Committee provided no information about the content of the classified information or how the Committee used it. The public version of the report does not describe that information in any way and does not cite it to support any particular finding, leaving no indication of its relevance or extent; though one can infer from the classified annex's stated purpose—"provid[ing] *significantly more information* adding to the Committee's concerns," *id.*—that it had a material impact. As discussed above, *supra* pp. 38-41, and below, *infra* pp. 81-82, classified material cannot play a critical role in an agency's factual determination against a party because that party would have no notice of the evidence used against it. *See People's Mojahedin Org.*, 613 F.3d at 231. The Commission cannot make an end run around the requirement that it disclose the evidence on which it relies simply by relying on a congressional report that also does not do so.

b. The HPSCI Report also borrowed indiscriminately from "expert" sources without making an independent evaluation as to their reliability or a rational connection to the Committee's assertions. As discussed below, *infra* at pp. 77-81, agencies can rely on expert reports when they are "well-reasoned" and "based on what is known and uncontradicted" by available evidence, *see Federal Power Comm'n*, 404 U.S. at 464, so long as they engage in an independent assessment, but an agency cannot put "inordinate faith in the conclusory assertions of an expert," *see Sea Robin Pipeline Co.* v. *FERC*, 795 F.2d 182, 188 (D.C. Cir. 1986). The trustworthiness of an agency's findings has "substantially diminished force when extended to the sources outside the investigative agency from which the agency culls the information for its report." *Brown* v. *Sierra Nev. Mem.*

Miners Hosp., 849 F.2d 1186, 1189-90 (9th Cir. 1988). Whether or not the Committee would be justified in its uncritical reliance on purported—and in many instances, unidentified—experts, that reliance does not provided evidence to support the Commission's assertions against Huawei.

The HPSCI Report also drew irrational connections from the reports it cited. For example, the Commission, parroting the HSPCI Report, claimed that when Huawei "seek[s] to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries." Order ¶ 56 (citing HPSCI Report at 2). But the HPSCI Report's support for this point is unsound. The HPSCI Report cites just a single source for this proposition—a National Institute of Standards and Technology ("NIST") draft paper that contains *not a single mention of Huawei*. *Id.* at 2 n.9 (citing NIST, *N[a]tional Supply Chain Risk Management Practices for Federal Information Systems*, NIST Interagency Report 7622, at 28 (Oct. 16, 2012)). Instead, the cited portion contains the unremarkable statement that "[e]lement and supply chain diversity can increase robustness against attack by reducing the likelihood or consequences of attack." NIST Report at 28. Further, the report states that "[a]n attack is less likely to succeed if diversity is implemented." *Id.* Nowhere in the paper is there any support for HPSCI's claim that Huawei "seek[s] to control the market," and in fact, Huawei submitted, under penalty, a statement to the Committee recognizing the merits of sourcing from different suppliers. *See* 2012 Huawei Cyber Security White Paper at 16 (submitted as Exhibit to 9/22/2012 Huawei Second Responses to HPSCI); *see also* 9/22/2012 Huawei Second Responses to HPSCI at 4.[14] The Committee ignored the evidence and instead drew

[14] Huawei has repeatedly affirmed its commitment to supply chain diversity and has submitted an expert report showing that banning Huawei from the US market actually decreases supply chain diversity, rather than increasing it. *See infra* pp. 90, 156-62. *See, e.g.*, Shampine ¶¶ 7, 13; Aron Report I ¶¶ 86-111; 11/12/2019 Huawei Ex Parte at 4-5; 2012 Huawei Cyber Security White Paper at 16; *see also* Aron Report II.

unsupported conclusions that advanced its political agenda. Compounding this error, the Commission then adopted this statement over seven years later as its own without giving it any apparent scrutiny.

Other key assertions in the report suffer the same infirmities. The report asserted that the "opportunities to tamper with telecommunications components and systems are present throughout product development, and vertically integrated industry giants like Huawei and ZTE provide a wealth of opportunities for Chinese intelligence agencies to insert malicious hardware or software implants into critical telecommunications components and systems." HPSCI Report at 3. But, to support this broad negative statement about Huawei, the report cited no evidence relating to Huawei or even China. The sole support proffered is a 2007 Defense Science Board report broadly claiming that the "means and opportunity are present throughout the supply chain and life cycle of software development" to "craft actionable malicious code mirrors" (though it did note one attack by hackers from China). *Id.* at 3 n.16 (citing Defense Science Board, *Report on Mission Impact of Foreign Influence on DoD Software* vii-viii (Sept. 2007) ("2007 Defense Science Board Report")); *see* 2007 Defense Science Board Report at 21-22. This general and conclusory statement (applicable to practically every telecommunications companies in the world) is insufficient to justify the Commission's specific designation of Huawei.

The HPSCI Report also makes unsupported claims about Huawei's founder, Mr. Ren Zhengfei, upon which the Commission then relied in turn. Citing only the HPSCI Report, the Commission stated that: "Huawei's founder, Ren Zhengfei, is himself believed to be a former director of the People's Liberation Army Information Engineering Academy, an organization associated with China's signals intelligence." Order ¶ 50 (citing HPSCI Report at 13-14). Despite the HPSCI's "extensive interviews" with Huawei on this point, HPSCI Report at 8, as well as an

interview with Mr. Ren himself, the HPSCI Report similarly cites no primary sources for its assertions about Mr. Ren's background and points to the beliefs of "many analysts," *id*. at 14; *but see* Ex. J, 7/3/2012 Huawei First Responses to HPSCI at 7-8 ("7/3/2012 Huawei First Responses to HPSCI"); 9/22/2012 Huawei Second Responses to HPSCI). But the cited source for the beliefs of these "many analysts" was a single RAND paper that provides no citation for the claim regarding Mr. Ren's background and that vaguely cites "Interviews in Beijing" for the claims regarding Huawei's purported connections to the government and military. *See id.* at 14 nn.40-41 (citing Evan S. Medeiros et al., *A New Direction for China's Defense Industry*, RAND Corp. 217-19 (2005)). The HPSCI Report's assertion regarding Huawei's connections to the Chinese government and military thus lacks meaningful support and cannot serve as a basis for the Commission's designation.

The report elsewhere cited statements from analysis of the Chinese political economy that "Huawei operates in what Beijing explicitly refers to as one of the seven 'strategic sectors.' … In these sectors, the [CCP] ensures that 'national champions' dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets." HPSCI Report at 21 & n.56. The source cited is not a team of analysts at all, but (once again) the non-neutral media op-ed supporting Australia's ban on Huawei, which itself cited no other sources. *See id.* at n.56 (citing John Lee, *The Other Side of Huawei*, *Business Spectator* (Mar. 20, 2012)). The report's assertion against Huawei in reliance on purported "analysts" therefore lacked an evidentiary basis. Moreover, it was directly contradicted by the sworn testimony of Huawei's Senior Corporate Vice President at the time, Charles Ding, who testified that he had no understanding of the term "national champion" and that Huawei had not been granted that title or any special privileges related to it. HPSCI Hearing at 23.

c. Finally, the HPSCI Report also based its assertions on an incorrect notion of Chinese law—namely, that Chinese laws obligate Huawei "to cooperate with "any" request by the Chinese government to use their systems or access them." HPSCI Report at 3 (emphasis added). Huawei explained to the Committee at the time that "no legislation in China that permits the Chinese government to use Huawei's equipment for national security or economic espionage or to force Huawei to use its equipment to engage in such espionage." 9/22/2012 Huawei Second Responses to HPSCI at 3. As discussed below, the HPSCI Report's reliance on an incorrect view of Chinese law cannot provide a basis for the Commission here to designate Huawei. *See infra* pp. 92-105.

c. The Commission erroneously relied on documents based on indictments as evidence against Huawei

The Commission also improperly rested its designation on two documents—the Commerce Department's Entity List and a letter from Attorney General Barr—that rely solely on unproven indictments as evidence of Huawei's guilt. That was error, because indictments are not evidence, and so the Commission may not rely upon them in its decisionmaking. *See, e.g.*, *United States* v. *Fattah*, 914 F.3d 112, 174 (3d Cir. 2019) (permitting the jury to receive a copy of the indictment only if "subject to a limiting instruction that the indictment does not constitute evidence, but is an accusation only"). Instead, by definition, indictments contain unproven allegations, not evidence of wrongdoing, and thus are "quite consistent with innocence." *Hurst* v. *United States*, 337 F.2d 678, 681 (5th Cir. 1964) ("[T]he fact of arrest or indictment is quite consistent with innocence, and [] the reception of such evidence is merely the reception of somebody's [hearsay] assertion as to the witness's guilt." (quoting Wigmore on Evidence III, 3d. Ed. § 980(a)); *United States* v. *Joyner*, 899 F.3d 1199, 1203 (11th Cir. 2018) (noting that trial judge twice instructed jury that "the indictment is not evidence of guilt"); *United States* v. *Esso*, 684 F.3d 347, 350 (2d Cir. 2012) (same);

United States v. *Anderson*, 174 F.3d 515, 524 (5th Cir. 1999) (same); *Scholes* v. *Lehmann*, 56 F.3d 750, 762 (7th Cir. 1995) (same); *see also* 1A Fed. Jury Prac. & Instr. § 13:04 (6th ed.); Model Crim. Jury Instr. 5th Cir. § 1.05 (2015) ("The indictment or formal charge against a defendant is not evidence of guilt. Indeed, the defendant is presumed by the law to be innocent."); Model Crim. Jury Instr. 3d Cir. § 1.11 (2018) ("An indictment is simply a description of the charge(s) against a defendant. It is an accusation only. An indictment is not evidence of anything.").

Although these cases arise from judicial proceedings, they apply with no less force here in the administrative context. The same reasons that compel courts to exclude indictments as evidence in judicial proceedings would render it patently unreasonable, and arbitrary and capricious, for an agency to rely on them as evidence in administrative proceedings. *See* 5 U.S.C. § 706(2)(A). At bottom, indictments are simply accusations unsupported by evidence; they are no substitute for any trial by evidence that might follow. Thus, indictments cannot provide an evidentiary basis for adverse agency actions. *Rivera* v. *Town of Huntington Hous. Auth.*, No. DRH-ARL-12-cv-901, 2012 WL 1933767, at *6-7 (E.D.N.Y. May 29, 2012) (holding that an arrest and pending charges were "not evidence" and "did not establish by a preponderance of the evidence that [the plaintiff] engaged in 'criminal activity'").

The Commission's reliance here on documents that in turn rely solely on indictments is no exception. *First*, the Commission cited the Commerce Department's Entity List (which does not even designate Huawei USA). Order ¶ 48. The *only* cited justification for Huawei's addition to the Entity List was an indictment in the U.S. District Court for the Eastern District of New York. *See* Addition of Entities to the Entity List, 84 Fed. Reg. 22961-01 (May 21, 2019). But the unproven accusations in that indictment are, of course, not evidence. Allegations in an indictment cannot

establish any fact of wrongdoing by a preponderance of the evidence in the proceedings the indictment initiated, let alone any facts in *these* proceedings. Accordingly, the Commission's reliance on Huawei Technologies' Entity List designation—which in turn relies solely on an indictment—is improper and cannot justify its designation of Huawei. *Second*, the Commission cited a letter from Attorney General Barr attributing to Huawei a "willingness to break U.S. law." Order ¶ 52 (quoting the Barr Letter at 2); *see also id.* ¶¶ 28, 45, 46, 62. But the *only* support Attorney General Barr offered for designating Huawei were two indictments and the Entity List, which itself relied solely on one of those indictments. *See* Barr Letter at 1. These indictments, like any indictment, contained only allegations, not evidence. *See Hurst*, 337 F.2d at 681. In any event, the Barr Letter itself conceded that "these cases [in which Huawei was indicted] do not discuss activities that would directly affect the security of our telecommunications networks." Barr Letter at 2. Accordingly, the Barr Letter cannot provide a basis for the Commission's designation of Huawei as a risk to telecommunications networks or the supply chain because it—along with the indictments upon which it relied—lacks probative value.

d. The Commission erroneously relied on unreliable hearsay as evidence against Huawei

Although hearsay may sometimes constitute evidence, a fundamental principle of our legal system is that hearsay lacking indicia of reliability should not be afforded evidentiary value. *Queen* v. *Hepburn*, 11 U.S. 290, 296 (1813) (Marshall, C.J.) ("[Hearsay's] intrinsic weakness, its incompetency to satisfy the mind of the existence of the fact, and the frauds which might be practiced under its cover, combine to support the rule that hearsay evidence is totally inadmissible."); *Chambers* v. *Mississippi*, 410 U.S. 284, 298 (1973) (noting that hearsay statements are "traditionally excluded because they lack the conventional indicia of reliability"). Consequently, courts have

recognized that hearsay must "bea[r] satisfactory indicia of reliability" to satisfy even the deferential substantial evidence test. *Crawford* v. *U.S. Dep't. of Agric.*, 50 F.3d 46, 49 (D.C. Cir. 1995); *Consol. Edison Co.*, 305 U.S. at 230 ("Mere uncorroborated hearsay or rumor does not constitute substantial evidence."); *EchoStar Commc'ns Corp.* v. *FCC*, 292 F.3d 749, 753 (D.C. Cir. 2002); *U.S. Pipe & Foundry Co.* v. *Webb*, 595 F.2d 264, 270 (5th Cir. 1979). In the context of congressional testimony, in particular, these principles require out-of-court statements to be "based upon an investigation made pursuant to legal authority" and contain "factual findings" based on reliable "data, facts, and conclusions" from "a legal investigation." *SEC* v. *Pentagon Capital Mgmt. PLC*, 722 F. Supp. 2d 440, 441-43 (S.D.N.Y. 2010) (quoting *Bridgeway Corp.* v. *Citibank*, 201 F.3d 134, 143 (2d Cir. 2000)).

The Commission relied on unreliable hearsay to support its designation of Huawei. To begin, the Commission relied on FBI Director Christopher Wray's congressional testimony expressing "dee[p] concer[n]" about "any company or entity that is beholden to foreign governments that don't share our values" and that "gain[s] positions of power inside our telecommunications networks that provides the capacity to exert pressure or control over our telecommunications infrastructure." Order ¶ 52 (citing Open Hearing on Worldwide Threats Before the SSCI, 115th Cong., at 64-65 (Feb. 13, 2018)). But as Wray's own words show, Wray's testimony reflected a general conclusion made only "at a 100,000-foot level"—a qualification the Commission failed to mention. Open Hearing on Worldwide Threats Before the SSCI, 115th Cong., at 64-65. Such general testimony lacks sufficient indicia of reliability to support the Commission's designation of Huawei. And nothing in Wray's testimony contained factual findings related to Huawei arising from a legally authorized investigation. In that sense, Director Wray's testimony was not evidence

at all, hearsay or otherwise, but rather naked opinion. The Commission therefore cannot rely on such testimony for its designation of Huawei. *Accord EchoStar*, 292 F.3d at 753.

The Commission also improperly relied on three congressional letters "express[ing] concern" about Huawei in its designation decision. Order ¶ 6 (citing Letter from Senator Jon Kyl et al. to Hon. Julius Genachowski, Chairman, FCC, Oct. 19, 2010 ("Kyl Letter"); Letter from Representative Anna Eshoo to Hon. Julius Genachowski, Chairman, FCC, Nov. 2, 2010 ("Eshoo Letter")); ¶ 11 (citing 12/20/2017 Cotton Letter).

The letters made several unwarranted accusations: Senator Kyl's letter asserted that Huawei was "financed by the Chinese government," is "potentially subject to significant influence by the Chinese military," and provides an "opportunity for manipulation of" telecommunication infrastructures. *See id.* ¶ 6. Representative Eshoo's letter criticized "foreign-controlled" suppliers of telecommunication equipment. *See id.* ¶ 6 n.4. And Senator Cotton's letter cited "the 2012 HPSCI Report" and asserted that Huawei must be "view[ed] with suspicion." *Id.* ¶ 11.

But the letters themselves are not evidence. And nothing they cited amounts to actual evidence either. The letters contained broad generalizations without factual basis and hearsay lacking indicia of reliability, not factual findings from a legally authorized investigation. *See Pentagon Capital*, 722 F. Supp. 2d at 442. Although Senator Kyl cited a "2009 report by the Department of Defense" and a "2005 report from the RAND Corporation" to support the notion that "Huawei has significant ties to the Chinese military" and "the People's Liberation Army" (Kyl Letter at 1), it is unclear what particular defense report he was referring to, and the RAND report (*see supra* p. 71), lacks reliability and probative value on this particular point.[15] And Representative Eshoo's letter

[15] Although offering no citation, Senator Kyl perhaps intended to refer to the Office of the Secretary of Defense, Annual Report to Congress: Military Power of the People's Republic of

rested exclusively on the "results of [a classified] assessment" by the Director of National Intelligence but failed to disclose any factual findings, asserting that "suffice to say the answers [in the classified assessment] were troubling." Eshoo Letter at 1. But the Commission cannot base its designation on undisclosed classified information without providing Huawei a meaningful opportunity to respond. *See supra* pp. 38-41; *infra* pp. 81-82. Finally, Senator Cotton's letter relied on the HPSCI Report, which, as discussed *supra* pp. 59-72, also lacks reliability. Such hearsay lacks probative value and thus cannot be part of the calculus showing that it is more likely than not that Huawei presents a national security threat, the touchstone of the Commission's action.

e. The Commission should not have relied on unreliable outside "expert" analysis, particularly since it did not perform its own independent and thorough review

The Commission relied on a number of outside expert reports. But the Commission was not permitted to rely on expert analysis without undertaking its own independent review of the reports. Although agencies may sometimes rely on outside analyses, *see Fed. Power Comm'n* v. *Fla. Power & Light Co.*, 404 U.S. 453, 464-65 (1972), such analyses cannot be used to support the agency's decision absent the agency's "own independent and thorough review," *Avoyelles Sportsmen's League, Inc.* v. *Marsh*, 715 F.2d 897, 907 n.17 (5th Cir. 1983), since "inordinate faith in the conclusory assertions of an expert" is insufficient, *Sea Robin Pipeline Co.*, 795 F.2d at 188. Moreover, even if the Commission conducts an independent and thorough review, the expert reports must still be reliable. The principle that experts should be qualified and use reliable methods clearly "plays a role in the administrative process because every decision must be supported." *Donahue* v. *Barnhart*, 279 F.3d 441, 446 (7th Cir. 2002). An expert report must be reliable and supported

China 2009 ("2009 Annual Report"). But only one sentence out of the entire 78-page report mentions Huawei—"Information technology companies, including Huawei, Datang, and Zhongxing, maintain close ties to the PLA and collaborate on R&D"—and that sentence omits any citation.

by factual evidence because an "expert who supplies nothing but a bottom line supplies nothing of value." *Mid-State Fertilizer Co.* v. *Exchange Nat. Bank of Chi.*, 877 F.2d 1333, 1339 (7th Cir. 1989); *White ex rel. Smith*, 167 F.3d at 375 ("Speculation is, of course, no substitute for evidence."); *cf. In re Scrap Metal*, 527 F.3d 517, 530 (6th Cir. 2008) (a court must decide whether an expert's opinion "rests upon a reliable foundation, as opposed to, say, unsupported speculation").

The Commission did not heed those principles here. There is no indication the Commission undertook such a review of the underlying materials cited by the "experts" it said it relied on. Indeed, had the Commission done so, it would have realized that the expert reports mostly consisted of unsourced rumors and hearsay. As discussed below, the bald assertions from the string of expert reports that all cite each other in a feedback loop fail to support the Commission's conclusions that Huawei possesses or has access to customer data, *see infra* pp. 147-49; works "with other firms to enable Chinese intelligence to impair communications privacy and exploit communications networks," Order ¶ 50; and has improper relationships with the Chinese government, *supra* pp. 64-71. As demonstrated *supra* pp. 66-68, the HPSCI Report is infected with hearsay. The other expert reports' reliance on the HPSCI Report, and other similar unsourced rumors and unsupported allegations, demonstrates that these reports constitute unreliable evidence that the Commission cannot use to support its designation. *Sea Robin Pipeline*, 795 F.2d at 188 (deeming "inordinate faith in the conclusory assertions of an expert" insufficient to support agency decisionmaking).

Moreover, the Commission relied on a series of expert reports to show that Huawei has security vulnerabilities in its equipment that the Chinese government is capable of exploiting. But, as discussed below, the Finite State Report relied on improper testing methods and the UK reports explicitly provide that their findings do not show hostile activity on the part of China. *See infra*

pp. 146-49. Simply put, all of these reports do not show it is more likely than not that Huawei poses a national security threat.

The Finite State Report, according to the Commission, described a purportedly "'high number' of security vulnerabilities" and purportedly found "at least one potential backdoor." Order ¶ 54 (citing Finite State, *Finite State Supply Chain Assessment* 3 (2019) ("Finite State Report")). But that report is deeply flawed and incomplete, as already and thoroughly explained by Huawei—for instance: (1) the report was a mere preliminary assessment; (2) Finite State assessed *outdated* versions of Huawei equipment; (3) Finite State's conclusions rested on the incorrect assumption that Huawei used Linux-based authentication; (4) Finite State failed to follow general practices of responsible testing companies, which typically involve dialogue between the security company and vendor about alleged vulnerabilities to help ensure a complete and accurate picture of security vulnerabilities; (5) Finite State provided no explanation of how it selected the vendors it used for purposes of comparison in its study, why it ignored the vendor who holds the largest market share of the global enterprise network, or why it tested almost all of the hundreds of Huawei enterprise network products, but only one product each of Juniper and Arista without disclosing the versions assessed; (6) Finite State incorrectly relied (among other things) on false reporting that Vodafone found an alleged "backdoor" in Huawei's equipment in Italy, but Vodafone had itself explained that the alleged backdoor was no backdoor at all and the issue was resolved in 2011 and 2012; and (7) none of Huawei products tested by Finite State will be deployed for 5G RAN or Core in telecommunications networks. *See* Ex. 16, 10/31/2019 Huawei Ex Parte (attaching a statement released by Huawei regarding the Finite State Report and a technical analysis of the Finite State Report performed by Huawei's Product Security Incident Response Team).

The Commission in its order failed to address any of these deficiencies. Where there are "specific challenges to [external] reports underlying [the] … analysis" that are "specifically and credibly challenged as inaccurate," the agency has an "independent duty to investigate." *Van Abbema* v. *Fornell*, 807 F.2d 633, 640 (7th Cir. 1986). The Commission failed to honor its duty. Instead, the Commission asserted that it "disagree[d]" with Huawei's analysis without addressing any of Huawei's "specific challenges" to the Finite State Report. *Id.* The Commission stated generally that "Finite State's report was a general risk analysis report and was focused primarily on the culture of risk management at Huawei." Order ¶ 57. But this vague assertion does nothing to address—let alone rebut—Huawei's challenges to the report's accuracy and reliability with respect to specific conclusions the report made about Huawei's equipment. The Commission's designation of Huawei was improper, in part because the Commission failed to acknowledge—let alone consider—any of Huawei's comments and evidence in the record showing that Huawei is a leader in developing robust cybersecurity standards that contribute to the integrity of its products.

The Commission also improperly relied on a report issued by the RWR Advisory Group in asserting that "Huawei is reported to be working with other firms to enable Chinese intelligence to impair communications privacy and exploit communications networks." Order ¶ 50 n.152 (citing RWR Advisory Group, A Transactional Risk Profile of Huawei at 16 (Feb. 13, 2018) ("2018 RWR Report")). But the report acknowledged, and in no way refuted, Huawei's statement that "[n]o solution or service [like that] has ever been incorporated into any Huawei product or service offered to any Huawei customer." 2018 RWR Report at 16. The report also relied on the HPSCI Report, which as discussed is unreliable (*supra* pp. 59-72), as well as on a political news source that in turn cited a purported Pentagon Paper that neither Huawei nor the public has access to. 2018 RWR Report at 16. The Commission improperly relied on the RWR Report again when it claimed

that "[w]hile Huawei has refused to answer questions about its ownership and governance, it can be inferred that the Chinese government clearly has a vested interest in the Company's success." Order ¶ 51 (citing RWR Report at 12). Neither the Commission nor the RWR posed these questions to Huawei. And when questions were posed by HPSCI, Huawei was responsive, *see* HPSCI Hearing; 7/3/2012 Huawei First Responses to HPSCI; 9/22/2012 Huawei Second Responses to HPSCI. Huawei has submitted ample documentation regarding its ownership and governance both before the Commission and now before the Bureau, *see supra* pp. 42-46; *infra* pp. 127-42. The report lacks reliability and Huawei's affirmative evidence shows it does not have material ties to the Chinese government.

f. The Commission should not have critically relied on classified information

The Commission improperly relied on classified information. Order ¶ 43 n.124 ("[T]he Commission has compiled and reviewed additional classified national security information that provides further support for our determinations."); Order at 108 (App'x E: Classified Supplement). Although the Commission asserted that the "publicly available information in the record is sufficient to support [Huawei's] designatio[n]," *id.* ¶ 43 n.124, that information, as explained, is itself based on nonevidence, unreliable evidence, or unwarranted inference, *see supra* pp. 56-82; *infra* pp. 82-105. And from the Order itself, it is clear that the Commission relied critically on classified information, since the publicly available sources it cited relied on classified information. *See, e.g.*, Order ¶ 44 & n.129 (citing HPSCI Report), ¶ 45 & nn.130-31 (same), ¶ 48 & n.144 (same), ¶ 50 & nn.148-49 (same), 151 (same), 152 (citing a report that relied on the HPSCI Report and a news source discussing a classified Pentagon Paper), ¶ 56 & nn.174-75 (citing HPSCI Report), ¶ 58 & n.186 (same). In particular, the Commission relied substantially on the HPSCI Report, which itself

contained a "classified annex" whose express purpose was to "provide *significantly more* information adding to the Committee's concerns." HSCPI Report at 10 (emphasis added). The Commission's suggestion that it did not critically base its designation on classified information cannot be sustained; accordingly, its use of such information was improper.

The Commission's preemptive defense of its critical use of classified evidence is unavailing. The Commission cited another agency order noting that "the Commission is legally empowered to receive classified national defense information and to use that information as the basis for a decision." Order ¶ 43 n.124 (citing *Policy to Be Followed in Future Licensing of Facilities for Overseas Communications*, Docket No. 18875, Order, FCC 78-756, 69 FCC 2d 1232, 1232 (1978)). But that order offered no authority for such a proposition. Instead, it cited the Commission's authorization to "withhold … secret information affecting the national defense." *Id.* As explained, however, that authorization does not permit the Commission to base its designation in a critical way on undisclosed classified information. Nor does the order address any of the authorities disallowing critical reliance on classified information without providing the regulated party a chance to respond. And neither *Bendix Aviation Corp.* v. *FCC*, 272 F.2d 533 (D.C. Cir. 1959), nor the Commission's decision in *China Mobile International (USA) Inc.*, 34 FCC Rcd. 3361 (2019) (*see* Order ¶ 43 n.124) addressed whether due process requires disclosure of classified information, relied on by an agency in a critical manner, to the regulated party or its counsel.

4. The Commission's conclusions are otherwise unsupported by evidence in the record, much less by a preponderance of the record evidence

As explained above, the Commission relied extensively on nonevidence and unreliable evidence to conclude that Huawei should be designated under its rule. When that nonevidence and unreliable evidence are set aside, there is insufficient evidence in the record to sustain the Com-

mission's designation decision. What little "evidence" the Commission pointed to is neither probative nor sufficient. The Commission could not, consistent with the APA's requirement of reasoned decisionmaking, rely on it to justify designating Huawei. The result is a designation that is not supported by any evidence, much less by a preponderance of the evidence.

a. The Commission does not support its assertion that the Chinese government and Communist Party control or exert influence over Huawei

The Commission designated Huawei in part based on its belief that the Chinese government and Communist Party "exert … influence on the company's operations and decisions." Order ¶ 43. But Huawei is a private company, which the Order does not contest, and it is not subject to Chinese government control. *See supra* pp. 42-46. The Commission fails to support each of its arguments in support of its claim that Huawei is subject to undue influence from the Chinese government.

First, the Commission claimed that the Chinese government and Communist Party can exert undue influence over Huawei because "Huawei's founder, Ren Zhengfei, is himself believed to be a former director of the People's Liberation Army Information Engineering Academy, an organization associated with China's signals intelligence." Order ¶ 50. But the Commission supported this bold assertion by citing *only* the HPSCI Report, *id.* ¶ 50 nn. 148-49, which as explained above, is not reliable on this point, even to the extent it may be termed evidence at all. *Supra* pp. 59-72. And, as Mr. Ren himself explained to the HPSCI (and explains again here, *see infra* pp. 131-34), he served in the military as a civil engineer working to establish a chemical fiber factory. *See* 7/3/2012 Huawei First Responses to HPSCI at 7-8; 9/22/2012 Huawei Second Responses to HPSCI at 7. Just as importantly, the Commission has not explained why prior military service permanently makes a veteran a presumed pawn of the government. Without any reliable or probative evidence to substantiate the Commission's assertions (let alone a reasoned explanation), it is irrational to suggest that the mere fact of Mr. Ren's prior military service makes him untrustworthy

or somehow beholden to the Chinese government. What is more, the Commission's fixation on Mr. Ren is puzzling. As Huawei has explained, he is not the only decisionmaker at Huawei. *See supra* p. 43.

Second, the Commission claimed that "the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions." Order ¶ 50. Again, the Commission supported this assertion with only a citation to the HPSCI Report, *id.* ¶ 50 n. 151, which is highly prejudicial and unreliable, *see supra* pp. 59-72. And the Commission ignored the reliable record evidence submitted by Huawei that Communist Party committees in private companies—required in all companies operating in China, including foreign-owned companies—do not and cannot exert influence over a company's operations and decisions. *See* deLisle Report at 6, 7 n.13, 18-19; Ye Decl. ¶ 30. The Commission did not cite to any admissible or reliable evidence to support its claim to the contrary.

Third, the Commission claimed that the Chinese state may exercise undue influence over Huawei because Huawei receives "vast subsidies from the Chinese government" and "it can be inferred that the Chinese government clearly has a vested interest in the company's success." Order ¶ 51. But the Commission cited no evidence for its assertion that Huawei is beholden to the government because it allegedly receives government funding. And it is irrational to make such an inference. Rather than being "vast," the figures are small compared to Huawei's revenues and expenditures. DeLisle Report at 9. Further, the types of government support to which the Commission points are common across the industry. *See id*. The FCC never compared the government support received by Huawei to the similar support received by its competitors, or analyzed whether any such support is provided on terms more favorable than Huawei could have obtained from commercial sources. Without such evidence, there is simply no basis to conclude that Huawei

receives any kind of competitive advantage or that Huawei would have any reason to be beholden to the government. In short, the Commission lacked any evidence to support its otherwise illogical inference that the Chinese government exerts undue influence over Huawei by allegedly providing it with immaterial amounts of common forms of support.

Fourth, the Commission appeared to conclude, as a predictive matter, that the Chinese government will ignore legal constraints in order to force companies like Huawei to spy for it. *See* Order ¶ 49 & n.146. But the Commission's conclusion is unsupported by the record. *See infra* pp. 83-88. As explained below, the proper interpretation of Chinese law is a question of law, and it is one that the Commission—no expert in foreign affairs or law—answered incorrectly. *See infra* pp. 91-105. And to the extent that the Commission alternatively suggested that the Chinese government might not follow Chinese law, it raised a question of fact, as Huawei's expert explained. *See* Chen Rebuttal to Clarke Memo ¶¶ 4.1, 8.1, 20.2, 24, 54 (whether the Chinese government is meaningfully constrained by Chinese law is "principally a matter of fact"). The Commission—here too no expert—thus bore the burden of proof on the issue, and it was obligated to consider the whole record and address "whatever in the record fairly detracts from" an agency's conclusion, *Universal Camera Corp.*, 340 U.S. at 488, including "contradictory evidence or evidence from which conflicting inferences could be drawn," *Lakeland Bus Lines*, 347 F.3d at 962 (quoting *Universal Camera Corp.*, 340 U.S. at 487). Further, the Commission's obligation to engage in reasoned decisionmaking included the duty to connect its predictions to a rational interpretation of the record. *See, e.g.*, *Int'l Ladies' Garment Workers' Union* v. *Donovan*, 722 F.2d 795, 822 (D.C. Cir. 1983) ("While we respect an agency's superior position to make judgments involving elements of prediction, we will review the record and the agency's decision to assure that it identified all relevant issues, gave them thoughtful consideration duly attentive to comments received, and

formulated a judgment which rationally accommodates the facts capable of ascertainment and the policies slated for effectuation." (quotation marks omitted)).

Despite its burden, the Commission pointed to no evidence that the Chinese government has asked Huawei, or any other company, to carry out malicious activities, or that Huawei would do so if requested. *See In re Universal Serv. Contribution Methodology*, 29 FCC Rcd. at 9719; *see also, e.g.*, Ex. S, *Huawei founder Ren Zhengfei denies firm poses spying risk*, BBC News (Jan. 15, 2019); 5/10/2019 Ex Parte at 4; 6/1/2018 Huawei Comments at 87 ("Huawei emphatically denies that it ever has, or would, tamper with its equipment or software at the behest of the Chinese government."); 2018 Huawei Annual Report at 5 (asserting that Huawei "strictly compl[ies] with all applicable laws and regulations in all the countries where we operate, including export control and sanction laws and regulations of the United Nations, the United States, and the European Union"). And as Huawei USA's Chief Security Officer attested, he has never encountered any inappropriate cooperation with, improper relationship involving, or undue influence by China. *See* Purdy Decl. ¶¶ 44-45. And Foreign Ministry Spokesperson Geng Shuang dismissed claims that Chinese law requires Chinese companies to coordinate with the Chinese government to steal secrets: "China has not asked and will not ask companies or individuals to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government by installing 'backdoors' or by violating local laws." Ex. R, *Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on February 18, 2019*, Ministry of Foreign Affairs of the People's Republic of China (Feb. 18, 2019); *see also* 5/10/2019 Huawei Ex Parte at 3.[16]

[16] Recent public statements by Chinese officials support the conclusion that the Chinese government will follow Chinese law. *See, e.g.*, Chen Rebuttal to Clarke Memo ¶¶ 60.1-60.4. For example, on March 15, 2019, Premier Li Keqiang told Bloomberg News: "You asked whether the Chinese government will ask Chinese companies to 'spy' on other countries. Let me tell you explicitly that this is not consistent with Chinese law. This is not how China behaves. China did not

Further, Huawei explained that there are well documented economic incentives for the Chinese government not to ask companies to spy for it. Indeed, as evidenced by its industry focus and investment actions, "[t]he predominant policy goal of Chinese party and state leaders for four decades has been economic growth." deLisle Report at 11-12. It is implausible that state leaders would use companies as vehicles for espionage and "put this multifaceted, high-priority, long-developing, much-invested-in agenda at risk." *Id.* at 13-16. Moreover, where an agency fails to adequately consider evidence in the form of expert opinions before it, its decision cannot survive review. *See, e.g.*, *Perez* v. *Mortg. Bankers Ass'n*, 575 U.S. 92, 96 (2015); *Mozilla Corp* v. *FCC*, 940 F.3d 1, 69-70 (D.C. Cir. 2019). Such a conclusion is especially problematic given that the Commission has neither national security expertise nor institutional responsibilities for making national security judgments.

Finally, the Commission based its designation of Huawei USA on a vague concern that the Chinese government might "exert" influence over Huawei's affiliates. Order ¶ 56, n.178. Again, the Commission placed no evidence in the record even suggesting that Huawei USA (or any other affiliate) has material ties with the Chinese government. *See supra* pp. 44-46.

In sum, after setting aside the unsupported inferences and unreliable evidence, the record lacks any evidence that the Chinese government and Communist Party "exert … influence on the company's operations and decisions." Order ¶ 43.

---

and will not do that in the future." Ex. N, Premier Li Keqiang Meets the Press: Full Transcript of Questions and Answers, State Council of the People's Republic of China (Mar. 15, 2019); *see* 5/10/2019 Huawei Ex Parte at 3.

b. The Commission did not support its assertion that Huawei's equipment contains security flaws, or explain why any flaws make it a national security threat to the integrity of communications networks or the communications supply chain

The Commission also failed to support its assertions that there exists a "multitude of evidence" of security flaws in Huawei's equipment, Order ¶ 56, or that even if such evidence existed, it would weigh in favor of designation. *First*, the Commission relied on comments submitted in the rulemaking proceedings by USTelecom. *Id.* ¶ 44 & n.126. But these comments do not cite any evidence; indeed, they cite the Commission's own NPRM as support for the assertion that Huawei's equipment contains security flaws. USTelecom Comments at 3 (citing NPRM ¶¶ 3-6). *Second*, the Commission cited the 2019 RWR Report. Order ¶ 44 & n.126. But this citation is misplaced because that report does not provide any support for the proposition that Huawei's equipment contains security flaws. Rather, the report states that it does not have evidence of a "*lack of* technical vulnerabilities." 2019 RWR Report at 4 (emphasis added). That backwards reasoning is no different from a presumption of guilt absent proof of innocence. *Third*, Huawei relied on the Finite State Report, which, Huawei has already explained, is deeply flawed and incomplete. *See supra* pp. 79-80. *Fourth*, Huawei cited the 2019 HCSEC Report and UK ISC Report, but these reports as a factual matter do not support the assertion that Huawei's equipment contains security flaws that threaten the United States' telecommunications networks and supply chain. *See supra* pp. 49-50. Indeed, the HCSEC has never found any malicious code or backdoor in Huawei's products. *See supra* p. 49.

Relatedly, the Commission also cited a NATO Cooperative Cyber Defence Centre of Excellence report for the general premise that China has a reputation for cyberespionage. Order ¶ 44 (citing NATO Cooperative Cyber Defence Centre of Excellence, *Huawei, 5G, and China as a Security Threat* at 7, 10 (2019) ("2019 NATO Report")). But even the Commission's own citation

ultimately betrays its conclusion about Huawei's security vulnerabilities. The report explicitly acknowledged that "there has been no evidence, at least publicly, of significant vulnerabilities in Huawei technology." 2019 NATO Report at 7. Because it exaggerates—or ignores—the various conclusions of the UK and NATO reports, the Commission is left without a basis to conclude that Huawei's products have security vulnerabilities in light of Huawei's evidence that its products are safe.

In all, the Commission provided no evidence that Huawei or Huawei USA has ever planted backdoors, eavesdropping devices, or spyware in its equipment, at the behest of the Chinese government or otherwise. By contrast, Huawei has repeatedly affirmed that it "has not planted and will not plant back doors to assist the national intelligence work or engage in the espionage activities." Chen Rebuttal to Clarke Memo ¶ 20. Indeed, Huawei founder and CEO Ren Zhengfei has stated that, even if the Chinese government were to ask Huawei to engage in cyberespionage, Huawei would never do so. *See, e.g.*, Ex. S, *Huawei founder Ren Zhengfei denies firm poses spying risk*, BBC News (Jan. 15, 2019). And the evidence before the Commission shows that Huawei adheres to rigorous cybersecurity practices, *supra* pp. 46-49, subjects its products to rigorous testing, *supra* pp. 49-51, and satisfies its customers' need for reliable and secure equipment, *supra* pp. 51-54.

Considering the Commission's failure to cite any reliable or probative evidence for its alleged "multitude" of security flaws, and the record evidence demonstrating Huawei's active commitment to cybersecurity practices and rigorous testing by oversight bodies, the Commission failed to rest its designation decision on evidence of the existence of equipment security flaws, much less a preponderance of the evidence.

c. The Commission did not support its assertion that Huawei's participation in the U.S. market threatens market diversity

The Commission asserted, with little explanation, that Huawei's "desire to be an end-to-end provider for whole network solutions" somehow threatens "market diversity" and "becomes a national concern for the United States and other countries." Order ¶ 56 (quoting HPSCI Report at 2). As an initial matter, the Commission failed to support that assertion with any reliable evidence. In any event, the Commission had it exactly backwards: More market participants means more market diversity, not less. As Huawei has demonstrated through its comments and record submissions, its presence in the United States is crucial for robust market competition. Huawei's entry and presence into the U.S. market would *improve* market diversity by giving consumers more choices in what is already a concentrated market. *See, e.g.*, Shampine Decl. ¶¶ 7, 13-23; Aron Report I ¶¶ 195-218. Thus, even crediting the statement that Huawei desires to be an end-to-end supplier, such a fact does not support the conclusion that Huawei presents a threat to communications networks or to the communications supply chain.

* * *

In sum, even assuming that the Commission put some "evidence" into the record, that evidence does not support the conclusion that Huawei should be designated. The Commission could not draw a rational connection between the evidence in the record and its conclusion that Huawei presents a national security threat to communications networks and the communications supply chain. The Commission could not show the substantial evidence required to survive judicial review, much less carry its burden of showing by a preponderance of the evidence that designation was warranted. And as shown below, the new evidence that Huawei submits in conjunction with these comments only further refutes the Commission's conclusions.

B. The Commission erroneously relied on unsupported conclusions about Chinese law that ignored Huawei's multiple expert submissions

The Commission's initial designation is also an impermissible basis on which to rest a final designation because it relied heavily on a misunderstanding of Chinese law to designate Huawei a national security threat to the integrity of the communications networks and the communications supply chain. One of the centerpieces of the Commission's designation of Huawei was the Commission's assertion that "Chinese laws obligat[e] [Huawei] to cooperate with any request by the Chinese government to use or access [its] system[]." Order ¶ 27. But the Commission itself has no expertise in Chinese law. And Huawei's multiple expert opinions explained that Chinese law does not in fact give the Chinese government independent authority to compel entities like Huawei to spy for it or otherwise carry out malicious cyber activities. The Commission's contrary conclusion invalidates the initial designation and provides yet another reason the Bureau may not rely on it.

1. The Commission was not permitted to base its initial designation of Huawei on legal error

An agency order "may not stand if the agency has misconceived the law." *SEC* v. *Chenery Corp.*, 318 U.S. 80, 87-90, 94 (1943). Thus, by expressly making its designation of Huawei turn on an interpretation of foreign law, the Commission left open the possibility that its construction of foreign law could be reversed on judicial review. That is because, "[j]ust like any question of law, '[t]he content of foreign law is a question of law and is subject to de novo review,"' and as a result, an agency receives "no deference" on its view of foreign law. *Iracheta* v. *Holder*, 730 F.3d 419, 423 (5th Cir. 2013). And an agency determination based on an agency's misapprehension of foreign law cannot stand: the longstanding general rule, on judicial review, is that reliance on a mistaken construction of law requires vacatur. *E.g.*, *Chenery*, 318 U.S. at 92-95.

In addition, the Commission was required to grapple with Huawei's arguments with respect to the important legal question of Chinese law. Failure to respond to comments on an important

issue—let alone failure to do so in a reasoned manner—will render the Commission's conclusion arbitrary and capricious. *See, e.g.*, *Perez*, 575 U.S. at 96 ("An agency must consider and respond to significant comments received during the period for public comment."); *Mozilla*, 940 F.3d at 69-70 (an agency must "respond to relevant and significant public comments" "in a reasoned way"); *Int'l Union, United Mine Workers of Am.* v. *Mine Safety & Health Admin.*, 626 F.3d 84, 94 (D.C. Cir. 2010) (holding that an agency's failure to address public comments made during the rulemaking proceeding "or at best its attempt to address them in a conclusory manner" was "fatal" to the agency's final rule); *Home Box Office, Inc.* v. *FCC*, 567 F.2d 9, 35-36 (D.C. Cir. 1977) ("Moreover, a dialogue is a two-way street: the opportunity to comment is meaningless unless the agency responds to significant points raised by the public."); *supra* pp. 38-42, 76-77, 81-82.

2. The Commission relied on its misinterpretation of crucial points of Chinese law to designate Huawei after failing to meaningfully consider Huawei's multiple expert submissions

The Commission misinterpreted Chinese law as allowing the Chinese government to require companies like Huawei to engage in cyberespionage. The Commission erred in two respects. *First*, the Commission failed to meaningfully consider Huawei's expert submissions on the meaning of Chinese law, and therefore acted arbitrary and capriciously. The Commission itself considers Chinese law to be a crucial consideration in its decision. *See* Order ¶¶ 27, 45-46, 48-49, 56. Indeed, it repeatedly stated that "Chinese laws obligating [Huawei] to cooperate with any request by the Chinese government to use or access [its] system, pose a threat to the security of communications networks and the communications supply chain." *Id.* ¶ 48; *see also id.* ¶ 27; *id.* at 109 (Statement of Chairman Pai). And during a hearing on May 7, 2019, Chairman Pai told the Senate Subcommittee on Appropriations: "I believe that certain Chinese suppliers, such as Huawei, do indeed present a threat to the United States, either on their own or because of Chinese domestic

law." Ex. T, John Eggerton, *FCC's Pai to Senate: Huawei is National Security Threat*, Broadcasting+Cable (May 8, 2019). Thus, any comments on the proper interpretation of Chinese law touch on—by the Commission's own words—an important aspect of the problem. And the Commission concedes that "the Chinese NIL may be interpreted in different ways." Order ¶ 56. Yet the Commission conducted only a cursory analysis of Chinese law and an even more cursory assessment of Huawei's expert submissions. For that reason alone, the initial designation is arbitrary and capricious and cannot stand.

Second, the Commission's flawed approach to Chinese law resulted in its misinterpretation of crucial provisions of Chinese law. The Commission relied on its misunderstanding of Chinese law as a critical consideration in its determination that Huawei poses a national security threat to the integrity of communications networks and the communications supply chain. As Huawei's experts explained, Chinese law *does not* permit the Chinese government to force companies like Huawei to spy for it. Because the Commission rested its designation of Huawei on a contrary interpretation of Chinese law, however, the designation cannot stand, and it cannot serve as a basis for any final designation by the Bureau.

a. Chinese law does not authorize the Chinese government to compel companies to engage in cyberespionage or other malicious cyber activity

Huawei's experts have explained that Chinese law does not permit the Chinese government to compel Huawei to spy for it. The Commission's contrary conclusion that Chinese law obligates Huawei to cooperate with the Chinese government in espionage and cyberattacks fails to take account of these expert opinions, and thus demonstrates a misunderstanding of China's national security laws. Relying on speculation in the HPSCI Report, the Commission asserts that Chinese law authorizes the Chinese government to "demand that private communications sector entities coop-

erate with any governmental requests, which could involve revealing customer information, including network traffic information." Order ¶ 46. But Huawei's experts have explained that the Commission's legal conclusion is mistaken, because Chinese law does not give the government independent authority to interfere in the operations of a privately owned and operated company like Huawei.

For example, Huawei's experts have explained that Article 13 of the Counterespionage Law[17] does not require Huawei to cooperate with the Chinese government in espionage and cyberattacks. That article provides that state security officials "may inspect and verify the electronic communication tools, apparatuses and other equipment and facilities of relevant organizations and individuals" "[a]s may be needed for counter-espionage work." 6/1/2018 Chen & Fang Decl. ¶ 14. Article 13 is "a typical administrative inspection provision" and its application is subject to "strict conditions." 5/10/2019 Zhou Report at 15. In particular, Huawei's experts explained, the law does not authorize national security organs to ask inspection objects to cooperate in law enforcement activities, monitor third parties, or engage in other acts that are detrimental to third parties. *Id.* at 16. And "Article 13 does not empower state security authorities to plant software backdoors, eavesdropping devices or spyware, or to compel third parties to do so." 6/1/2018 Chen & Fang Decl. ¶ 7.

Furthermore, Article 13 applies only to "relevant organizations and individuals who own, hold or use electronic communication tools, devices, and other equipment or facilities." *Id.* ¶¶ 18-19. "[R]elevant organizations" include "Chinese institutions, organizations, and individuals[,] and institutions or organizations established by parties from foreign countries or regions, including

[17] The HPSCI Report expressed concern about the former State Security Law, which has since been superseded by the Counterespionage Law of 2014. *See* 6/1/2018 Chen & Fang Decl. ¶¶ 11-21, 24.

Chinese-funded enterprises, China-foreign joint ventures and cooperative enterprises, and solely foreign invested enterprises." *Id.* The inspected targets "are traditionally major channels and tools engaged in espionage activities and harmful to national security," "not … telecommunication equipment manufacturer[s] such as Huawei, let alone an overseas subsidiary or organization belonging to Huawei." 5/10/2019 Zhou Report at 16; 6/1/2018 Chen & Fang Decl. ¶ 21; *see id.* ¶¶ 7, 18-19. Moreover, before state security authorities may act pursuant to Article 13, they must have "explicit counterespionage purposes, and clear and specific goals or targets of counterespionage." 6/1/2018 Chen & Fang Decl. ¶ 17. The Chinese government may not act pursuant to Article 13 based on nothing more than "uncertain and general goals to protect state security." *Id.* Thus, Huawei's experts have explained that, contrary to the concerns raised in the HPSCI Report, Article 13 provides no legal authority for the Chinese government to compel Huawei to spy for it.

None of the other laws implicated by the HPSCI Report or cited by the Commission would require Chinese telecommunications companies to engage in espionage and cyberattacks on behalf of the Chinese government either. For example, Article 18 of the Anti-Terrorism Law provides that "[t]elecommunications business operators and Internet service providers shall provide technical interfaces, decryption and other technical support and assistance for public security organs and State security organs to prevent and investigate terrorist activities in accordance with the law." 6/1/2018 Chen & Fang Decl. ¶ 26 (quoting *PRC Anti-Terrorism Law*, Article 18). Huawei's experts have explained that this provision would not authorize the Chinese government under any circumstances to order telecommunication equipment *manufacturers* to hack into their own products. *Id.* ¶ 8. In fact, Article 18 applies only to telecommunication service providers and internet service providers; it does not apply to telecommunication equipment manufacturers like Huawei

USA. *Id.* And even telecommunication and internet service providers are exempt from the obligations of Article 18 unless the national security authorities are seeking "to prevent and investigate terrorist activities." *Id.*

Similarly, Huawei's experts have explained that Article 28 of the Cyber Security Law does not provide a legal basis for the Chinese government to compel telecommunication equipment manufacturers to spy on its behalf. That law directs that "[n]etwork operators shall provide technical support and assistance" to state security authorities "in the activities of protecting national security and investigating crimes in accordance with the law." *Id.* ¶ 50 (quoting *PRC Cyber Security Law*, Article 28). To begin with, Article 28 applies only to network operators—including Chinese subsidiaries of U.S. companies. But Huawei is a manufacturer of telecommunications equipment, not a network operator. *Id.* ¶ 9; Chen & Fang Supp. Decl. at 5 ("[The] identification of network operators depends on the actual nature and content of the service and products they provided."); *see also* Chen Rebuttal to Clarke Memo ¶ 56 (identifying the limited reach of this statute as not applying to businesses that merely operate "their [own] internal network"). Huawei is therefore outside the scope of the requirements of Article 28. Moreover, the legislative purpose of the Cyber Security Law is "to ensure China's cyber security, not to threaten or endanger the security of any other country's networks." 6/1/2018 Chen & Fang Decl. ¶ 9. Article 28 thus, by its terms, does not empower the Chinese government to require private companies to engage in espionage on its behalf.[18]

[18] Further, if a private company attempted to engage in these activities on its own, it would violate a separate provision of the Cyber Security Law. *See, e.g.*, Chen Rebuttal to Clarke Memo ¶ 70.1 ("Article 27 of the PRC Cyber Security Law provides that, any individual or organization shall neither engage in activities endangering cyber security, including illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data, nor

Nor do any other provisions of Chinese law compel Huawei to allow Chinese intelligence agencies to take control of its communications systems or to plant backdoors or spyware in telecommunications equipment, or to require Huawei to do the same. In its Order, the Commission found that Articles 7, 14, 17, and 28 of the Chinese NIL together would enable the Chinese government to take control of Huawei USA's communications systems to engage in espionage. *See* Order ¶ 46. But Huawei's experts have explained that none of those provisions, or any others the Commission cites, would authorize such conduct or otherwise permit the Chinese government or its officials to require telecommunications equipment manufacturers to plant backdoors or spyware into telecommunications equipment. Indeed, Huawei's experts have explained that China's "[n]ational security authorities and public security authorities do not have any statutory powers to plant backdoors, eavesdropping devices, or spyware in equipment manufactured by Huawei, and Huawei has no obligation to cooperate with any such government request." 6/1/2018 Chen & Fang Decl. ¶ 65; *see also id.* ¶ 80 ("Requiring a telecommunication equipment manufacturer to plant backdoors, eavesdropping devices, or spyware that would be used to spy on or disable communications of its customers would directly contradict … the Constitution of China.").

More specifically, Article 7 states that an organization "shall, in accordance with the law, support, assist and cooperate with national intelligence work." 6/1/2018 Chen & Fang Decl. ¶ 70 (quoting *National Intelligence Law* Article 7). Article 14 similarly provides that an intelligence agency "may, when carrying out intelligence work pursuant to the law, require relevant organs, organizations and citizens to provide necessary support, assistance and cooperation." *Id.* (quoting *National Intelligence Law* Article 14). But neither provision applies outside China, so neither has

provide programs or tools specifically used for activities endangering cyber security, such as network intrusions, interference with the normal functions and protective measures of the network, and theft of cyber data.").

any bearing on Huawei's U.S. operations. *Id.* ¶¶ 73, 75, 77. And even if those articles did apply to Huawei, both provisions explicitly state that any requests for cooperation from the national intelligence agencies shall be "in accordance with the law." *Id.* ¶ 78; *see also* Chen Rebuttal to Clarke Memo ¶ 70; 8/6/2018 Chen & Fang Supp. Decl. at 3-4. This requirement is not mere boilerplate language. Huawei's experts explained that, in the Chinese Civil Law system, the phrase "in accordance with the law" means that "the scope of such requirement must be codified into law before becoming a legal obligation for organizations and citizens"—that is, some provision of law must provide an affirmative authorization or obligation. 6/1/2018 Chen & Fang Decl. ¶ 78. But there is currently no Chinese law in effect that would authorize the Chinese intelligence agencies to require a telecommunications equipment manufacturer to plant backdoors, eavesdropping devices, or spyware in its equipment. *Id.* Thus, any request by the government that a company engage in such activities would be unlawful.

Article 17 similarly does not authorize the Chinese government to take control of an organization's communications equipment. That article provides that the staff of national intelligence agencies, when necessary for their work, are entitled to "preferential use of, or [to] lawfully requisition, transport vehicles, communications tools, premises or buildings of relevant organs, organizations, and individuals" and to "set up relevant work sites, equipment and facilities." 11/1/2019 (Zhou Supp. Report ¶¶ 1, 3 (quoting *PRC National Intelligence Law*, Article 17)). Neither of these two clauses would allow an intelligence agency to take control of a company's telecommunications infrastructure. To begin with, Huawei's experts have explained that the FCC Denial Order incorrectly translated "communications tools" into "communications equipment." The term "communications tools" under Chinese law does not refer to "telecommunication facilities such as switches, servers, and routers." *See id.* ¶ 3. And because Article 17 applies only within

Chinese territory, it has no bearing whatsoever on Huawei's U.S. operations. *Id.* ¶ 4. Thus, nothing in the text or application of Article 17 would allow intelligence officials to access Chinese telecommunication facilities produced by Huawei in China, much less its U.S. telecommunication facilities.

Furthermore, any obligations that private companies might have under Articles 7, 14, and 17 of the NIL are purely defensive. In other words, "[t]hese obligations are applicable only when acts that endanger China's national security are conducted." 5/10/2019 Zhou Report at 3, 7. Companies do not have "general, unconditional, or offensive obligations." *Id.* at 3. And because "Huawei's participation in building communications networks outside China does not endanger China's national security," "China's national intelligence agencies cannot use [the NIL] to require Huawei to implant 'backdoors' in its equipment or … to help China's national intelligence agencies intercept or destroy the communications networks of other countries." *Id.* at 3, 5.

Finally, the Commission misrepresents Article 28. Huawei's experts have explained that that provision of the NIL allows national intelligence agencies to recommend punishment when an individual or entity obstructs their intelligence work. 11/1/2019 Zhou Supp. Report ¶ 6. As its text suggests, Article 28 is concerned with parties who "obstruct" the law, a term that "generally involves an intentional effort to hinder law enforcement through violence, threatening, or other acts." *Id*. Parties are not necessarily subject to legal liability for mere noncompliance. *Id.* Moreover, Article 28 alone cannot establish criminal liability, because Chinese law instead requires crimes to be defined in the Criminal Law, and China's Criminal Law has no provision establishing criminal liability for failing to cooperate with intelligence agencies. *Id.* The only intelligence-related crimes covered by China's Criminal Law relate to stealing state secrets or intelligence. *Id.*

The Criminal Law clearly would not apply to an entity's failure to build backdoors in telecommunication equipment.

The Commission also based its designation of Huawei, in part, on its conclusion that "the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions." Order ¶ 50. But Huawei's experts have explained that the Commission's conclusion that the Chinese government exerts substantial control over Huawei's business decisions is unfounded. *See supra* pp. 42-46; *infra* pp. 127-146. Communist Party committees do not have the right to interfere with company decisionmaking in a private company like Huawei. Ye Decl. ¶¶ 9-15, 28-30. And Chinese law recognizes private enterprises as legally independent from the Chinese government. *See, e.g., id.* ¶¶ 15-19, 23-24, 42-45. Chinese law specifically protects the autonomy of private businesses from government and third-party interference. *See id.* ¶¶ 42-45 (providing examples of Chinese legislation and regulations that protect private contracts and other private activities from governmental interference). In fact, Chinese law explicitly prohibits civil servants from interfering in the decisionmaking of private companies. *Id.* ¶¶ 46-49 (providing examples of such laws). And Chinese law imposes harsh punishments on officials who violate these laws. *Id.* ¶ 50. These punishments are consistent with the Constitution of China as well as case precedent, in which the Supreme People's Court of China has upheld "the inviolable right of companies to manage their own affairs." *Id.* ¶¶ 35-41.

Nor do the Communist Party's own internal Rules and Code of Conduct provide a basis for the Chinese government to interfere with the decisionmaking of private companies. The Rules and Code of Conduct of the Chinese Communist Party recognize that Chinese law "protects the rights of enterprises' autonomy of operation" and set forth penalties for any persons responsible

for "interference in the autonomy of the people in production and management." *Id.* ¶¶ 55-58 (citing Chinese Communist Party Disciplinary Regulations (rel. Oct. 21, 2015), Article 106; Decision of the Central Committee of the Communist Party on Several Major Issues Concerning Ruling the Country in Accordance with Law, 4th Plenary Session of the 18th Central Committee of the Communist Party of China (Oct. 23, 2014)). In addition, Communist Party Disciplinary Regulations explicitly state that "as a matter of policy, [the Party] should not interfere with the autonomy of businesses." *Id.* ¶ 56. There is therefore nothing in Chinese law, the rules of the Communist Party, or Huawei's own governing documents that would allow the Chinese government to intervene in Huawei's business decisionmaking either directly or indirectly. *Id.* ¶ 59. Huawei provided expert testimony that, while the Communist Party does establish organizations within private enterprises in order to facilitate meetings and communications between its members, "such organizations have no legal basis to interfere in a private company's operations or business decisions." *Id.* ¶ 14. Indeed, it is "straightforward and not controversial" that "there is no legal basis for the PRC government to interfere in the decision-making of any privately owned enterprises or companies." *Id.* ¶¶ 13, 29, 68.

The Commission also ignored the Chinese government's repeated public statements that the NIL does not empower the government to take control of private telecommunications equipment. For example, a senior official of the Standing Committee of the People's Congress recently clarified that "situations [for] using the provisions to plant backdoors or encroach on enterprise intellectual properties … do not exist." 6/1/2018 Chen & Fang Decl. ¶ 42. Similarly, on February 16, 2019, Yang Jiechi, a senior member of the Communist Party of China, stated that China does not have any laws that require companies to collect foreign intelligence. *See* 5/10/2019 Huawei Ex Parte at 3; *see also* Ex. Q, *Yang Jiechi: Hope the United States (US) Side Will Work with the*

Chinese Side to Well Implement the Consensus of the Two Heads of State and Promote Bilateral Relations Based on Coordination, Cooperation and Stability, Embassy of the People's Republic of China in the United States of America (Feb. 17, 2019).[19]

b. The Chinese laws at issue do not apply extraterritorially

Even if the foregoing provisions of Chinese law compelled Chinese companies to assist the government in espionage—and Huawei's experts have explained that they do not—they do not and cannot constrain the conduct of Chinese companies' overseas subsidiaries. Huawei's experts have further explained that Chinese law does not apply to any of the Huawei subsidiaries located outside of China, including Huawei USA. In particular, the NIL—with which the Commission was primarily concerned, *see* Order ¶ 46—does not apply to Huawei's subsidiaries and employees outside of China. *See* 6/1/2018 Chen & Fang Decl. ¶ 84; 5/10/2019 Zhou Report at 12. For example, Article 17 of the NIL is applicable "only within Chinese territory, and does not require subjects outside of China to fulfill legal obligations according to Chinese law." 11/1/2019 Zhou Supp. Report ¶ 4. Nothing in this provision would allow Chinese intelligence officials to access telecommunications facilities in the United States or would require Huawei USA's assistance in such an endeavor. *See id.* The same is true for NIL Articles 7 and 14. *See* 6/1/2018 Chen & Fang Decl. ¶ 10. In fact, the only provision of the NIL that even mentions extraterritorial scope is Article 10,

[19] Since the initial designation, high-ranking Chinese officials have reiterated these points. Foreign Ministry Spokesperson, Geng Shuang, explained that "[n]o law in China has required companies to install backdoors or collect foreign intelligence." Ex. O, Transcript, *Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on December 17, 2019*, Ministry of Foreign Affairs of the People's Republic of China (Dec. 17, 2019). And the Chinese Ambassador to the United Kingdom, Liu Xiaoming, further clarified "[t]he fallacy that China's National Intelligence Law could 'force' telecommunications suppliers to hand over data to China is nothing but scaremongering, not least because this law stipulates that 'national intelligence work shall be carried out in a way that respects and protects human rights, and safeguards the legitimate rights and interests of individuals and organisations.'" *See* Ex. P, *Banning Huawei would leave Britain trailing behind on technology*, Telegraph (Jan. 4, 2020).

but that provision merely defines the function of the national intelligence agencies and does not implicate private organizations or citizens. *Id.* ¶ 74. Similarly, Article 28 of the Cyber Security Law, Article 13 of the Counterespionage Law, and Article 18 of the Anti-Terrorism Law do not apply to Huawei's overseas subsidiaries. *See id.* ¶¶ 7-9. Accordingly, the Chinese laws that the Commission cited to support Huawei's designation do not even apply to Huawei's U.S. operations.

The Clarke report's contrary conclusion—on which the Commission relied to support Huawei's initial designation, *see* Order ¶ 49—is flawed, speculative, and unsupported. To begin with, the Clarke report concedes that Chinese state security laws "regulate only Chinese entities *and do not apply to Huawei's overseas subsidiaries*." Chen Rebuttal to Clarke Memo ¶ 20 (emphasis added). In other words, the Clarke Report concedes its own premise and instead assumes that Chinese enforcement authorities would violate Chinese law to force Huawei to pressure its overseas subsidiaries to assist in China's national intelligence work. But that assumption is not an interpretation of Chinese law. Instead, it is a prediction unsubstantiated by the Commission's failure to point to any evidence in the record. And the Commission, as concededly *not* a "[n]ational security [or] law enforcement agenc[y]," has neither expertise nor evidence to conclude otherwise. Order ¶ 19. Furthermore, the Clarke Report's conclusion that the Chinese government is unrestrained by Chinese law is undermined by the opinions of several Chinese legal experts. *See* Chen Rebuttal to Clarke Memo ¶¶ 12, 20. Moreover, the Chinese government itself has repeatedly emphasized that Chinese companies should "strictly abide by local laws and regulations when doing business overseas," and it has confirmed that China "has not asked and will not ask companies or individuals to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government by installing back doors or by violating local laws." *Id.* ¶ 20.3. The Clarke report's conclusions to the contrary are factually unsupported, and the report

thus cannot provide a sufficient factual basis to conclude that Huawei's overseas subsidiaries are bound by Chinese law.[20]

c. Chinese law provides procedural requirements and restrictions on law enforcement designed to prevent such abuse

Huawei's expert reports have also pointed out that the Chinese legal system imposes constraints on law enforcement authorities that are designed to prevent them from interfering with companies' legal rights and interests. The NIL in particular contains several provisions designed to safeguard the rights and interests of individuals and organizations. Pursuant to Article 8 of the NIL, all national intelligence agencies "shall … respect[] and safeguard[] human rights, and safeguard[] the legitimate rights and interests of individuals and organizations." 6/1/2018 Chen & Fang Decl. ¶ 71 (quoting *PRC National Intelligence Law*, Article 8). Article 19 similarly provides that "[a] National Intelligence Work Agency and its staff members shall not … infringe upon the legitimate rights and interests of citizens and organizations." *Id.* (quoting *PRC National Intelligence Law*, Article 19). If such infringement occurs, Article 31 of the NIL provides that "such actions are to be disciplined by the law, including subject to criminal prosecution." *Id.* The Commission's assumption that the Chinese legal system "recognizes no limits to government power" is inaccurate. Order ¶ 49 & n.146 (quoting Clarke Report at 3). Huawei's experts have explained that there are legal constraints on government power and legal provisions providing rights of action to enforce those constraints. *See* Chen Rebuttal to Clarke Memo ¶ 16. If national security authorities attempted to violate the NIL by requiring telecommunications equipment manufacturers to plant backdoors in equipment, the PRC Administrative Procedure Law provides for an avenue to seek

[20] Moreover, the Commission ignores the fact that many of the engineers and other Huawei employees that serve customers in the United States, including those that receive USF support, are American citizens or permanent residents, or citizens of allies of the United States. *See* 6/1/2018 Purdy Decl. ¶ 6; 6/1/2018 Dowding Decl. ¶ 3; Danks Decl. ¶ 4.

judicial relief against such actions. *See id.* ¶ 8.2; *see also id.* ¶ 12.2 (validating the fundamental use of this judicial relief: "the PRC Supreme People's Court" has issued "over 2.3 million administrative judgments so far"). For example, Article 2 of the Administrative Procedure Law "provides that, where citizens, legal persons, or other organizations" believe that government acts or officials "have infringed their legitimate rights and interests, they shall have the right to institute proceedings in [the] people's courts." *Id.* ¶ 8 n.4. Similarly, Article 12 of that law provides that citizens and organizations shall have the right to bring a lawsuit if they "believe that administrative authorities ask[ed] them to perform duties in contravention of the law." 6/1/2018 Chen & Fang Decl. ¶ 23. And Article 44 of the Administrative Procedure Law empowers the people's court to review the government's decisions and revoke them if they are determined to be unlawful. *Id.*; *see* Ye Decl. ¶¶ 31-34.

* * *

In sum, the Commission's reliance on Chinese law was legal error. The Commission rested its designation of Huawei on its conclusion that Chinese law authorizes the Chinese government to require Huawei to spy for it. But the Commission has no expertise in Chinese law; Huawei's experts have explained that Chinese law provides no such authorization and instead requires the Chinese government to respect the autonomy of businesses like Huawei; and the Commission failed to explain the basis upon which it rejected these expert views as incorrect. Accordingly, the Commission's views about Chinese law cannot serve as a basis for designating Huawei—not by the Commission, and not by the Bureau.

C. The Commission's decision to selectively target Huawei was arbitrary and capricious

By designating Huawei but not similarly situated companies a national security threat to the integrity of communication networks and the communications supply chain, the Commission

acted irrationally, and so its designation decision cannot stand. It is well settled that "an agency's unjustifiably disparate treatment of two similarly situated parties works a violation of the arbitrary-and-capricious standard." *LePage's 2000, Inc.* v. *Postal Reg. Comm'n*, 674 F.3d 862, 866 (D.C. Cir. 2012) (per curiam) (quotation marks omitted). An agency thus "must give a reasoned analysis to justify the disparate treatment of regulated parties that seem similarly situated, and its reasoning cannot be internally inconsistent." *ANR Storage Co.* v. *FERC*, 904 F.3d 1020, 1024 (D.C. Cir. 2018) (citation and quotation marks omitted). "Where an agency applies different standards to similarly situated entities and fails to support this disparate treatment with a reasoned explanation and substantial evidence in the record, its action is arbitrary and capricious and cannot be upheld." *Burlington N. & Santa Fe Ry. Co.* v. *Surface Transp. Bd.*, 403 F.3d 771, 777 (D.C. Cir. 2005); *see also Melody Music, Inc.* v. *FCC*, 345 F.2d 730, 732-33 (D.C. Cir. 1965).

The Commission singled out Huawei and ZTE from the beginning of these proceedings, with no apparent intent of ever designating other companies. Indeed, the cost-benefit analysis for the rule focused only on the costs and benefits associated with banning Huawei and ZTE. Order ¶¶ 108-21. And, as explained below, the Commission's targeting of Huawei was the product of congressional pressure and prejudgment. *See infra* pp. 114-20. In any event, the Commission has given no such reasoned analysis for its disparate treatment of Huawei. Consequently, the designation is arbitrary and capricious and unlawful.

The Commission failed to explain why other similarly situated companies are not security risks, but Huawei is. The Commission merely asserted that Huawei poses a "unique" threat to security because of (1) its size, (2) security flaws in its equipment, (3) its design and manufacturing processes, (4) its close relationship with the Chinese government, (5) obligations imposed by Chinese law, and (6) the end-to-end nature of Huawei's service agreements. Order ¶ 45. But other

telecommunications companies share these same attributes. These characteristics are not unique to Huawei, as Huawei has repeatedly explained to the Commission. *See, e.g.*, Suffolk Decl. at 2-5; Exs. 1-M, 1-N; Exs. 3-E to 3-M; Exs. 14-A to 14-II; deLisle Report 9-10, 17-19; 8/6/2018 Chen & Fang Decl. ¶¶ 34-39, 48, 55-62, 75-77, 84; *see generally* 8/6/2018 Huawei Ex Parte; 9/18/2019 Huawei Ex Parte. The Commission has proffered no "reasoned analysis" to justify its disparate treatment of Huawei. *ANR Storage Co.*, 904 F.3d at 1024.

First, the Commission's assertion that Huawei's size was the basis for designation is irrational. The Commission asserted that "Huawei and ZTE pose a unique threat to the security of communications networks and the communications supply chain because of their size." Order ¶ 45. But Samsung's annual revenue in 2018 was double Huawei's, yet the Commission chose not to designate Samsung under the rule. *See* Aron Report I App'x ¶¶ 1, 5, 8-10. Moreover, Huawei's revenue in 2018 ($107 billion) was an order of magnitude larger than ZTE's ($12.7 billion), so it is irrational for the Commission to suggest that Huawei and ZTE are uniquely similar in size. *See id*. The Commission has not attempted to explain why Huawei and ZTE—which have dramatically different annual revenues—were targeted for their size, while Samsung, which is far larger than both Huawei and ZTE, was not.

Second, the Commission provided no reasoned explanation for basing its designation of Huawei on alleged security flaws in Huawei's equipment. Order ¶ 45. The Commission never asserted—much less *proved*—that Huawei's equipment contains security flaws greater than those present in the equipment produced by any other major telecommunications company. And the "widespread consensus" is that, given the complex and global supply chain, it is "not possible to eliminate all cybersecurity risk." 7/2/2018 Purdy Supp. Decl. ¶ 8. Huawei has readily acknowledged, and continues to mitigate, the "upstream" and "downstream" supply chain risks associated

with "maliciously tainted products and counterfeit products." 2016 Huawei Cyber Security White Paper at 10-11; *see also* 2012 Huawei Cyber Security White Paper at 5-8; Suffolk Decl. at 4-5. But every telecommunications company that participates in the global supply chain faces these risks, *see id.*, and the Commission does not explain how or why Huawei is unique in this respect.

Moreover, even if Huawei's equipment had more security flaws than equipment produced by other participants in the global supply chain (and the Commission did not rely on such an assertion), it would not be enough for designation. The Commission failed to explain why Huawei's equipment would create a greater national security threat to the integrity of communication networks and the communications supply chain than equipment produced by other telecommunications companies. Indeed, Huawei submitted a report on supply chain vulnerabilities prepared by Interos Solutions, Inc., for the U.S.-China Economic and Security Review Commission of the U.S. Government ("Interos Report"), which deems three Dell and Microsoft suppliers—not Huawei—as "present[ing] the most risk to the supply chain" as a result of their "close ties to Chinese government entities, particularly entities involved in China's military, nuclear, or cyberespionage programs." Ex. 14-II, Interos Solutions, Inc., *Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology*, at 15 (Apr. 19, 2018) ("Interos Report").[21]

Third, the Commission suggested that Huawei's "design and manufacturing processes" in China pose a risk to U.S. security, but it failed to explain why other telecommunications companies with significant operations in China do not pose a comparable risk and why they have not also

[21] Huawei relies on the Interos Report for the limited point that the Commission fails to explain its disparate treatment of similarly situated entities. Huawei does not agree with the Report's assumption that substantial relationships with Chinese entities constitute security risks to the telecommunications networks of other countries, and Huawei strongly denies any allegations—which the report concedes are based on "unconfirmed reports"—about intellectual property theft. Interos Report at 25. Huawei also does not agree with any of the other critical assertions about Huawei that appear in the Interos Report.

been designated. For example, the Commission chose not to designate Nokia as a covered company, even though Nokia also has obvious ties to China. Nokia has "six Technology Centers, one regional Service Delivery Hub, and more than 80 offices" in China. Ex. 14-G, Nokia Corp. Form 20-F 2017 (submitted as Ex. 7 to 9/18/2019 Huawei Ex Parte). And Cisco, as Huawei explained, "has a huge presence in China, with R&D centres in six major cities." 2012 Huawei Cyber Security White Paper at 9. Indeed, "[o]ver 25% of all Cisco products are produced by Chinese partners, and the company announced a US$16 billion investment in China that includes training 100,000 network engineers and the opening of 300 centres at vocational colleges to train students in networking technologies." *Id.* And, in fact, "*every* major telecommunications equipment provider has a substantial base in China." *Id.* at 9-10 (emphasis added; providing Nokia and Ericsson as examples); *see also* Ex. 14-R (Hewlett Packard maintains "Product Development, Services and Manufacturing" facilities in China); Ex. 14-T (Lenovo (Xian) Limited, a Chinese-foreign equity joint venture, provisions IT services and distributes IT products for Lenovo); Exs. 14-X, 14-Y (Alpha Networks conducts R&D, manufactures, and sells out of mainland China), Ex. 14-Z (Arista Networks sources a number of required communications components for their products from China), Ex. 14-AA (Extreme Networks "conduct[s] supply chain management, quality assurance, manufacturing engineering and document control" at its facility in China), Ex. 14-BB (Juniper Networks is dependent on Chinese manufacturers), Exs. 14-CC to 14-EE (BBK Electronics Corp, manufacturer of Oppo, Vivo, OnePlus, and Realme smartphones, is a Chinese company), Exs. 14-FF to 14-HH (Tsinghua Unigroup, third-largest smartphone chipmaker, manufactures heavily in China).[22]

In short, the distinctions between Huawei and non-Chinese firms are irrational. At a bare minimum, the Commission offered no reasoned explanation required to satisfy the APA. Relevant

[22] These exhibits were previously submitted as exhibits to the 9/18/2019 Huawei Ex Parte.

vulnerabilities can be introduced at any point in the supply chain and equipment made by a non-Chinese company that includes parts manufactured in China may contain the same relevant components about which the Commission might be concerned. *See* deLisle Report at 17-19. Huawei raised these issues before the Commission, but the Commission failed to respond to its concerns about disparate treatment. *See* 6/1/2018 Huawei Comments at 39-41. In fact, the Order did not even attempt to explain why other similarly situated companies with ties to China—like Nokia—have received more favorable treatment than Huawei.

Fourth, the Commission stated that its "concerns center around Huawei's established relationship with the Chinese government." Order ¶ 48. But even assuming that the Commission's concerns rested on some evidence of such a relationship, *but see supra* pp. 42-46, 59-72, 77-81, 83-88, the Commission failed to explain why it did not designate other telecommunications companies that have dealings with the Chinese government. For example, the Commission did not explain why it chose not to designate Nokia, which *united in a joint venture* with the Chinese government: Nokia Shanghai Bell Co. *Id.*; *see also* Suffolk Decl. at 2 (noting that "Nokia has a joint venture with a Chinese Government-owned entity, Nokia Shanghai Bell"); Ex. 1-M, "Nokia Signing a Joint Venture Agreement with China Huaxin to Establish Nokia Shanghai Bell" (submitted as Ex. M to 6/1/2018 Huawei Comments). Unlike Huawei, which the Order does not contest is a private company, Nokia Shanghai Bell is directly supervised by the State-Owned Assets Supervision and Administration Commission of the State Council. *See* Ex. 1-N, "Nokia 2016 Corporate Social Responsibility Report of Shanghai Nokia Bell" (submitted as Ex. N to 6/1/2018 Huawei Comments). Based on the Commission's stated concerns about companies with an "established relationship" with the Chinese government, the Commission's disparate treatment of Huawei and Nokia—a company with a joint venture with the Chinese government—is irrational. Indeed, absent

congressional pressure, unconstitutional prejudgment, and ex parte contacts with Nokia, *see supra* pp. 23-24; *infra* pp. 114-24, there is *no* apparent explanation for, on the one hand, the Commission's persistent, strained, and baseless efforts to show that the Chinese government might exercise some form of influence over Huawei, and, on the other hand, the Commission's decision to ignore evidence of Chinese state ownership of and control over the affiliate of a major competitor. The APA's reasoned decisionmaking requirement does not permit agencies to irrationally signal out particular entities in this manner.

In addition, the Commission contended that "the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions." Order ¶ 50. But every company operating in China—including U.S.-based companies—are required to permit the operation of a Party organization by its employees. Ye Decl. ¶ 28; deLisle Report ¶¶ 18-19; WTO Report ¶ 1.9. And other telecommunications and technology companies, including Huawei's competitors, have Party organizations or committees. *See, e.g.*, Ex. 3-H, "Enterprise Party Organization Oriented Toward Directing, Team Building, and Atmosphere Fostering" (submitted as Ex. H to 8/6/2018 Huawei Comments) (discussing Nokia Shanghai Bell's Party committee).

Moreover, to the extent the Commission alleged that the Chinese government exerts influence over Huawei by providing it with government support, *see supra* pp. 84-85, the Commission fails to distinguish Huawei from the numerous other technology companies who receive similar government assistance. For instance, Huawei explained that the credit line available to Huawei customers from the China Development Bank derives from an export-promotion program not dissimilar from those provided by the United States' Export-Import Bank and other export-promotion

programs funded by other governments around the world. deLisle Report at 8-9. Huawei's competitors, including Ericsson, Samsung, and Nokia, all participate in this program and receive similar benefits. *See id.* Had the Commission engaged in reasoned decisionmaking about any evidence about the government support Huawei allegedly receives, it would have come to the conclusion that any support the Chinese government provides to Huawei is unremarkable and indistinguishable from that provided to its peers that were not designated.

Fifth, to the extent the Commission was concerned with the applicability of Chinese law to Huawei, Order ¶ 45, the Commission has failed to explain why other companies who do business in China—and who are thus subject to the same laws as Huawei—are not similarly suspect under the rule. Huawei is not subject to additional legal obligations beyond those imposed on other companies that do business in China. In fact, any obligations that Huawei would have under the NIL are the same as those of other organizations or citizens residing in China, including Chinese subsidiaries of U.S. companies. 6/1/2018 Chen & Fang Decl. ¶ 10. As Huawei's experts explained, "[t]here is no difference between an organization owned by Chinese shareholders (such as Huawei), and an organization owned by non-Chinese shareholders (such as a subsidiary of a foreign manufacturer in China), in terms of their obligations under the National Intelligence Law, which simply does not distinguish based on the ownership of organizations in Articles 7 and 14." *Id.* ¶ 77. Chinese subsidiaries of U.S. companies are thus subject to the very same legal obligations as Huawei. 8/6/2018 Chen & Fang Suppl. Decl. ¶ 6 ("[T]he legal obligations of Huawei under the Cyber Security Law and the National Intelligence Law are the same and not more than that of any foreign-funded ICT companies residing in China.").

Accordingly, even if the Commission were correct in its interpretation of Chinese law—and it is not—the Commission acted arbitrarily and capriciously by refusing "to explain its different treatment" of Huawei as compared to nearly all other companies doing business in China purportedly subject to the same Chinese laws. *Melody Music*, 345 F.2d at 732. Similarly, to assert more broadly (as the Commission does) that the Chinese government will disregard the legal constraints imposed on it and thus may compel Huawei to act on its behest through extra-legal political means does not justify designation either. Order ¶ 49 & nn.146-47 (citing NATO Cyber Defence Centre Paper at 11; Mannheimer Swartling, *Applicability of Chinese Intelligence Law to Chinese and non-Chinese Entities* at 3 (2019)). That rationale would apply just as much to other companies doing business in China or with a parent company in China, and thus cannot support singling out Huawei for designation. By designating Huawei under the rule and failing either to designate Nokia or to provide a reasoned explanation of the disparate treatment of the two companies, the Commission has violated the "fundamental norm of administrative procedure" that "an agency [must] treat like cases alike." *Westar Energy, Inc.* v. *FERC*, 473 F.3d 1239, 1241 (D.C. Cir. 2007).

Sixth, the Commission's decision to target Huawei based on its "desire to be an end-to-end provider," even though several other companies already serve as end-to-end providers, constituted disparate treatment. Order ¶ 56. Without any explanation, the Commission assumed that Huawei's desire to be an end-to-end solution provider was motivated by a "desire to limit diversity in equipment," which the Commission concluded is a risk to national security. *Id*. The Commission did not, however, make the same assumptions about Nokia, Ericsson, and Samsung, all of whom currently provide end-to-end solutions. Ex. 14-S, "Magic Quadrant for LTE Network Infrastructure" (submitted as Ex. 19 to 9/18/2019 Ex Parte) (comparing "10 vendors of end-to-end (radio access

and core) infrastructure for LTE networks"). If Huawei's desire to provide end-to-end whole network solutions constitutes a risk to national security, then surely the fact that these three companies currently act as end-to-end providers poses an even greater risk. Indeed, the Commission provided no explanation to the contrary.

Under each of these considerations, the Commission has treated Huawei disparately from other similarly situated companies and has offered no explanation for this differential treatment. This error alone requires vacatur of Huawei's designation. *Melody Music*, 345 F.2d at 732 (agency's "refusal at least to explain its different treatment" was error).

D. The designation was infected by unconstitutional congressional pressure and unconstitutional prejudgment against Huawei

As its arbitrary and capricious nature suggests, the Commission's initial designation of Huawei was not the result of an objective, evidence-based analysis. Instead, that initial designation resulted from (1) pressure from members of Congress placed on the Commission, in violation of Huawei's due process rights, and (2) the Commissioners' unconstitutional prejudgment that Huawei posed a national security threat. These corrosive features of the Commission's decisionmaking violated Huawei's due process rights and, as noted, culminated in an arbitrary and capricious decision to target Huawei without any notice, any ascertainable criteria, or any rationale for why Huawei was treated differently from similarly situated companies.

In short, the Commission engaged in a wholly unprecedented process in order to presumptively (really, conclusively) designate Huawei. It employed a bait-and-switch in which an adjudication was tacked on to a rulemaking at the last minute, denying Huawei any notice that such a designation was even possible—indeed, misleading Huawei by affirmatively stating that the Commission was considering a "rule," not an adjudication. This rush to judgment without any process is extraordinarily suspicious, because it is both facially unfair and blatantly unnecessary: if there

really were evidence of Huawei's guilt, the Bureau would have so found in the process used for all others, free of the dispositive pressure conveyed by the Commission's "confident" conclusions that Huawei is guilty, as is the process established under the USF rule for all other designations of designated companies moving forward. *See* Order 66 (to be codified at 47 C.F.R. § 54.9(b)(1)) (directing the Bureau—not the Commission—to make the initial determinations of whether a company poses a national security threat). This facially suspicious rush to judgment, coupled with an extraordinarily explicit dialogue between Chairman Pai and Congress concerning Huawei's preordained guilt, demonstrates that the Commission's process was irreparably tainted with externally imposed and biased prejudgment, or at least the clear appearance thereof.

1. The Commission unconstitutionally singled out Huawei for initial designation based on political demands from members of Congress

An administrative adjudication is "invalid if based in whole or in part on [congressional] pressures." *D.C. Fed'n of Civic Ass'ns* v. *Volpe*, 459 F.2d 1231, 1246 (D.C. Cir. 1971); *see also ATX, Inc.* v. *U.S. Dep't of Transp.*, 41 F.3d 1522, 1527 (D.C. Cir. 1994) (same). Indeed, in judicial and quasi-judicial administrative proceedings, congressional "pressure is sufficient, standing alone, to invalidate [an agency's] action," regardless of whether that pressure actually affected the agency's decision. *D.C. Fed'n of Civic Ass'ns*, 459 F.2d at 1245; *see also Peter Kiewit Sons' Co.* v. *U.S. Army Corps of Eng'rs*, 714 F.2d 163, 169 (D.C. Cir. 1983) ("[P]ressure on the decisionmaker alone, without proof of effect on the outcome, is sufficient to vacate a decision."). That is because congressional pressure on an agency's judicial or quasi-judicial determination "sacrifices the appearance of impartiality—the sine qua non of American judicial justice." *Pillsbury Co.* v. *FTC*, 354 F.2d 952, 964 (5th Cir. 1966). And even when an agency is exercising a non-judicial function, congressional communications unconstitutionally infect the proceeding if they "actually influence[] the agency's decision"—that is, if "'extraneous factors intrude[] into the calculus of

consideration' of the individual decisionmaker." *DCP Farms* v. *Yeutter*, 957 F.2d 1183, 1188 (5th Cir. 1992) (quoting *D.C. Fed'n of Civic Ass'ns*, 459 F.2d at 1246)).

Here, the Commission's decisions to designate Huawei—and its decision to promulgate a USF rule that served as a vehicle to single out Huawei and ZTE under the guise of a generally applicable rule—were tainted by congressional interference, in violation of Huawei's Fifth Amendment due process rights. At a bare minimum, the designation *appears* to have been influenced by congressional pressures, and for that reason alone, it cannot stand.

The record of congressional pressure and interference is compelling. On December 20, 2017, eighteen members of Congress sent Chairman Pai a letter expressing their "concern[] about Chinese espionage in general, and Huawei's role in that espionage in particular." Letter from Senator Tom Cotton, *et al.*, U.S. Senate, to Hon. Ajit Pai, Chairman, FCC (Dec. 20, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-349859A2.pdf. The members emphasized the HPSCI Report's conclusion that "Huawei … cannot be trusted to be free of foreign state influence and thus poses a security threat to the United States and to our systems." *Id.* Based on that conclusion, they asked the Commission to review the relationship between Huawei and a certain U.S. telecommunications provider. *Id.* The members also advised the Commission of the HPSCI Report's recommendation that "U.S. government systems … should not include Huawei or ZTE equipment" and that "government contractors … should exclude ZTE or Huawei equipment in their systems." *Id.* The letter closed by asking "whether employees of the FCC are currently permitted to use Huawei products in the conduct of government business." *Id.*

This letter drove the Commissioners' decision to designate Huawei as a covered company—and even to promulgate the USF rule in the first place, which (as noted) was a transparent attempt to target Huawei and ZTE under the guise of a generally applicable rule. *See also supra*

pp. 8-9. After receiving the letter, Chairman Pai personally replied to those eighteen members of Congress, stating that "[he] share[d] [their] concerns about the security threat that Huawei and other Chinese technology companies pose to our communications networks." 3/20/2018 Pai Letter. Chairman Pai also assured those members of Congress that he would take action in response to their concerns: "At your suggestion … I intend to take proactive steps to help ensure the integrity of the communications supply chain in the United States in the near future." *Id.* Less than a month later, the Commission released the NPRM that led to the USF rule. *See generally* NPRM. And senior Commission officials have confirmed that the proposal to ban USF recipients from using "suspect Chinese tech" was prompted by pressure from members of Congress. *See, e.g.*, Ex. T, John Eggerton, *FCC's Pai to Senate: Huawei is National Security Threat*, Broadcasting+Cable (May 8, 2019) ("According to senior FCC officials speaking on background, the proposal stemmed, in part, from a Dec. 20, 2017, letter from Congress expressing concerns about Chinese companies Huawei and ZTE … .").

The text of the Order confirms that congressional pressure shaped the Commission's decision to fashion a rule targeting Huawei and to proceed simultaneously to designate Huawei under that rule. *See Koniag, Inc., Vill. of Uyak* v. *Andrus*, 580 F.2d 601, 610 (D.C. Cir. 1978) (stating that it is "[a] more serious matter" where congressional pressure may have actually affected an agency's decision); *ATX*, 41 F.3d at 1528 (noting that courts are most "concerned when congressional influence shapes the agency's determination of the merits"). The Order explicitly cites the congressional communications that the Commission received regarding Huawei. *See, e.g.*, Order ¶ 6 (October 2010 letter from lawmakers to the FCC Chairman expressing concern about Huawei); *id.* ¶ 11 (December 2017 letter from eighteen Senators and Representatives to Chairman Pai regarding Huawei). It also repeatedly cites the HPSCI Report that condemns Huawei as a national

security threat (even while it concedes that it cannot prove that conclusion, *see supra* pp. 64-65). *See, e.g.*, Order ¶¶ 7 & n.5, 11, 30 n.87, 35 n.106, 44, 45. And it explicitly cites section 889 of the 2019 NDAA as a basis for the rule and for its decision to target Huawei: The Order explains that section 889 expresses Congress's view that "the role of the Commission … is to prevent the use of federal funds under [its] control on equipment and services from [] suppliers of concern," and that its rule and "initial designation of Huawei" are "consistent" with Congress' expectations. Order ¶ 38 (quotation marks omitted). The Commission's explicit reliance on these congressional communications makes clear that extraneous pressure from Congress influenced the Commission's decision to target Huawei. *See D.C. Fed'n of Civic Ass'ns*, 459 F.2d at 1248 (explaining that, where an agency bases its decision "on the pressures generated by [Congress] … it should be clear that [the agency's] action would not be immunized merely because [it] also considered some relevant factors"); *see also ATX*, 41 F.3d at 1529 (suggesting that, where an agency's final decision explicitly mentions the congressional communications at issue, such a fact can constitute "evidence that the legislative activity *actually* affected the outcome on the merits").

Furthermore, and importantly, Chairman Pai was not remotely "non-committal in [his] reactions to the congressional contacts" he received regarding Huawei. *ATX*, 41 F.3d at 1529. He did not advise them that he was engaged in an adjudication, and "stress[] that it was inappropriate for him to discuss the merits of the case with the congressmen." *Id.* To the contrary, he assured the members of Congress that he would take prompt action against Huawei to address their concerns. *See* 3/20/2018 Pai Letter. The Commission Chairman's explicit promise to yield to congressional pressure is compelling evidence of an adjudicatory process infected by politics. Indeed, Chairman Pai's correspondence with the eighteen members of Congress alone "compromised the appearance of the [Commission's] impartiality." *Koniag*, 580 F.2d at 610-11 (finding that a single letter from

one congressman to the Secretary of the Interior "compromised the appearance of the Secretary's impartiality" in an adjudication and required reversal of the agency's decision). And when the Commission released the Order, Chairman Pai wrote separately that the Commission had "take[n] these actions based on evidence in the record"—*but see supra* pp. 56-82—"as well as *longstanding concerns from the executive and legislative branches* about the national security threats posed by certain foreign communications equipment manufacturers, most particularly Huawei and ZTE." Order at 109 (Statement of Chairman Pai) (emphasis added).

Several members of Congress also issued public statements before and during the Commission's proceedings that increased the pressure on the Commission to take action against Huawei. For example, on August 1, 2018, Senator Marco Rubio told his fellow legislators:

> If we can't even take on ZTE because they lobby and because of American companies coming here, how are we ever going to take on Huawei or any other dangers they pose to us? It is time we open our eyes. We are engaged in a geopolitical competition … with a global superpower that is quickly nipping at our heels and doing so unfairly, with the intent of replacing us in the world as its most powerful country militarily, economically, geopolitically, and technologically.

115 Cong. Rec. S5541 (daily ed. Aug. 1, 2018) (statement by Sen. Rubio). Similarly, on February 7, 2018, Senator Tom Cotton stated that "Huawei is effectively an arm of the Chinese government, and it's more than capable of stealing information from U.S. officials by hacking its devices … . There are plenty of other companies that can meet our technology needs, and we shouldn't make it any easier for China to spy on us." Ex. U, Press Release, Cotton and Rubio Introduce Legislation to Prohibit U.S. Government Use of Chinese Telecommunications Companies (Feb. 7, 2018). And on October 8, 2012, the Chairman of the House Intelligence Committee, Mike Rogers, stated: "[W]e have serious concerns about Huawei and ZTE, and their connection to the communist government of China. China is known to be the major perpetrator of cyber espionage, and Huawei and

ZTE failed to alleviate serious concerns throughout this important investigation. American businesses should use other vendors." Ex. V, Press Release, Ruppersberger, Rogers Warn U.S. Companies Doing Business With Huawei, ZTE (Oct. 11, 2012). Statements such as these reflect Congress's pervasive and consistent hostility toward Huawei, which contributed to the pressure on the Commission to single out Huawei for disparate treatment.

2. The Commission deprived Huawei of its Fifth Amendment right to a fair and impartial decisionmaker because several Commissioners had already prejudged Huawei's case

The pressure Congress placed on the Commission had its desired effect: Before issuing the rule and designating Huawei under it, several Commissioners had already prejudged Huawei to be a national security threat. Their involvement in Huawei's designation therefore deprived Huawei of its due process right to a fair and impartial decisionmaker. To determine whether an adjudicatory proceeding has been infected by prejudgment bias, in violation of the Fifth Amendment and the APA, a court must ask "whether a disinterested observer may conclude that (the agency) has in some measure adjudged the facts as well as the law of a particular case in advance of hearing it." *Cinderella Career & Finishing Schools, Inc.* v. *FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970) (quotation marks omitted) (due process); *see also Valley* v. *Rapides Par. Sch. Bd.*, 118 F.3d 1047, 1052 (5th Cir. 1997); *Latecoere Int'l, Inc.* v. *U.S. Dep't of Navy*, 19 F.3d 1342, 1356 (11th Cir. 1994), *as amended* (May 27, 1994) (asserting that "predetermining" the issues or "harboring a prejudice against" a party "generally constitutes arbitrary and capricious action") (APA). Here, the public record is replete with evidence that several Commissioners had long made up their minds about Huawei and thus could not fairly judge Huawei under the APA or the Fifth Amendment.

While this proceeding was pending before the Commission, several Commissioners made public statements showing that they had already made up their minds that Huawei should be targeted. For example, during a hearing on May 7, 2019, Chairman Pai told the Senate Subcommittee

on Appropriations: "I believe that certain Chinese suppliers, such as Huawei, do indeed present a threat to the United States, either on their own or because of Chinese domestic law." Ex. T, John Eggerton, *FCC's Pai to Senate: Huawei is National Security Threat*, Broadcasting+Cable (May 8, 2019). Similarly, on October 28, 2019, Commissioner Brendan Carr tweeted a *Wall Street Journal* article by Chairman Pai entitled "FCC Answers The Threat From Huawei" and commented: "I have no doubt that China intends to spy on persons and businesses within our borders. We must secure our telecom networks from this threat. I'm glad we're acting on the rip and replace proposal that I first discussed last year." Ex. W, Brendan Carr (@BrendanCarrFCC), Twitter (Oct. 28, 2019, 12:34 PM). Chairman Pai and Commissioner Carr's statements that Huawei is a threat to national security "can only be interpreted as a prejudgment of the issue." *Antoniu* v. *SEC*, 877 F.2d 721, 723 (8th Cir. 1989).

Commissioner Geoffrey Starks also made numerous public statements during the pendency of the proceeding that revealed he had prejudged Huawei's guilt. For example, on May 26, 2019, Commissioner Starks wrote an article in which he stated that "Huawei's equipment contains software vulnerabilities that could seriously compromise our network security," and that "[t]he Federal Communications Commission must find this equipment and work with other policymakers to fix the security problems and fund a solution for affected carriers." Starks, *The Huawei threat is already here*. When asked in an interview whether there is anything Huawei could do to get Commissioner Starks' trust back or to fix the situation, Commissioner Starks stated that it would be "very hard" for Huawei "to mitigate" these issues. Patel & Kelly, *FCC Commissioner Geoffrey Starks talks Huawei and net neutrality on the Vergecast*. And on June 22, 2019, Commissioner Starks stated: "The thing that I'm really focused on right now is coming up with solutions for

dealing with Huawei and other risky equipment that's already in our networks." Reardon, *FCC commissioner wants Huawei gear out of US networks*.

Commissioner Starks even held a stakeholder "workshop" that sought "to find untrustworthy and insecure communications equipment … , fix the problems posed by this equipment, and help fund the process." Security Vulnerabilities Within Our Communication Networks, Report of the Stakeholder Workshop Held June 27, 2019 at the Federal Communications Commission (Nov. 21, 2019), https://docs.fcc.gov/public/attachments/DOC-360931A1.pdf (emphasis omitted). Commissioner Starks's report on the workshop is replete with references to Huawei and suggests that Huawei should be targeted. *See e.g.*, *id.* at 1 ("China is using Chinese manufacturers like Huawei and ZTE as instruments in its efforts to achieve 5G dominance"); *id.* at 2 (asserting that Huawei software has "front doors" accessible by "bad actors"); *id.* at 2-3 (stating that "finding insecure or untrusted equipment" requires "determining where Huawei, ZTE, or other untrustworthy equipment is located"); *id.* at 14-15 (estimating costs to replace Huawei and ZTE equipment). There is no question that a disinterested observer would conclude, based on these public statements, that Commissioner Starks had "in some measure adjudged the facts as well as the law of [Huawei's] case in advance of hearing it" and that "the ultimate determination of the merits [would] move in predestined grooves." *Cinderella*, 425 F.2d at 590-91.

The direct and repeated attacks on Huawei by the ultimate decisionmakers in this proceeding left "no room for a determination that there was a decision by a fair tribunal, with the appearance of fairness." *Staton* v. *Mayes*, 552 F.2d 908, 914-15 (10th Cir. 1977). These public statements did more than merely "call[] attention to the pending proceedings." *Cinderella*, 425 F.2d at 589. Instead, they revealed to the public that at least a majority of the Commissioners—Chairman Pai

and Commissioners Carr and Starks—had already decided to target Huawei, regardless of the comments they received during the notice and comment period. In fact, Commissioner Starks essentially said as much when he commented that it would be "very tough" for Huawei to regain his and the U.S. government's trust. Patel & Kelly, *FCC Commissioner Geoffrey Starks talks Huawei and net neutrality on the Vergecast*. This statement leaves no doubt that Commissioner Starks had "demonstrably made up his mind about important and specific factual questions and [wa]s impervious to contrary evidence." *Fogo de Chao (Holdings) Inc.* v. *DHS*, 769 F.3d 1127, 1148 (D.C. Cir. 2014). At the very least, the Chairman's and Commissioners' statements "give the appearance that [they] ha[d] already prejudged the case." *Cinderella*, 425 F.2d at 590.

Furthermore, because Chairman Pai and Commissioners Carr and Starks all participated in Huawei's designation proceeding, "there is no way of knowing" precisely how their "participation affected the [Commission's] deliberations." *Antoniu*, 877 F.2d at 726. But the rule and designation indisputably appear to have "move[d] in predestined grooves," *Cinderella*, 425 F.2d at 590, and the Commission's suggestion that it dutifully fulfilled the role Congress had prescribed for it, *see* Order ¶ 38, confirms that the outcome of the proceedings was preordained. The Commission's invocation of national security, *see, e.g.*, Order ¶ 48, does not cure that violation. "It requires no superior olfactory powers to recognize that the danger of unfairness through prejudgment is not diminished by a cloak of self-righteousness" based on "the public interest." *Cinderella*, 425 F.2d at 590.

The Commission's prejudgment is evident in the expectations that the Order sets out for the Bureau's next steps. Even though the Order formally contemplates a final designation decision by the Bureau, it leaves no doubt that the Commission believes that the ultimate step is ministerial. The Commission's cost-benefit analysis for the underlying rule analyzed estimates and purported

data pertaining only to the exclusion of Huawei and ZTE—and no other entities. Order ¶¶ 108-21. The Commission clearly expects that Huawei and ZTE will be excluded—as the fact that the Commission itself entered initial designations against them confirms. The die has been cast. Unless the Commission expects its cost-benefit analysis to be *completely* off target, *cf.* Order at 112 (Statement of Commissioner O'Rielly), then it must anticipate that the purported costs and benefits it discussed will materialize because the Bureau will obligingly enter a final designation of Huawei.

* * *

For all the reasons discussed above, the Commission rested its designation of Huawei on legal errors and either ignored or failed to adequately address the affirmative evidence that Huawei submitted during the rulemaking. Properly assessed, the record makes clear that the Commission could not rationally justify designating Huawei as a risk to the telecommunications networks and supply chain. Such a designation cannot be supported by a preponderance of actual, reliable record evidence (*see supra* pp. 36-105). The Commission's designation was based instead on nonevidence, unreliable evidence, legal error, and irrational and unconstitutional prejudgment. The initial designation should be reversed and the Bureau should terminate these proceedings.

II. The Bureau should not enter a final designation against Huawei

The Bureau should not enter a final designation against Huawei for the same reasons the Commission should not have—and then some more. To begin with, the initial designation rested on legal and evidentiary error, as well as arbitrary and capricious reasoning and unconstitutional congressional pressure and prejudgment. Any one of those reasons—and certainly all of them together—invalidates the initial designation and eliminates it as a basis for any final designation. What is more, the same legal requirements discussed above apply to the Bureau's designation determination: The Bureau must base its determination on the record as a whole (without ignoring any evidence that contradicts its preferred outcome); must make rational connections between the

evidence and the facts found; and must not rest any designation on nonevidence, unreliable evidence, or other legal error. Failing to heed those requirements, the Commission manifestly came to the wrong conclusion on the record before it. And there is no reason to expect the record to support designation now any more than it did before. Final designation would therefore be wholly improper. But that is not all: Huawei now submits additional evidence demonstrating that the Commission's concerns—its apparent ad hoc considerations under its standardless rule—are unsubstantiated.[23]

A. The Bureau cannot rest a final designation on the Commission's initial designation, and it cannot make the same mistakes the Commission made in the initial designation

1. The Commission's invalid initial designation cannot support a final designation by the Bureau

As explained above, the Commission had to show that designation of Huawei was warranted by a preponderance of the evidence. The Commission failed to make anything remotely approaching such a showing. Instead, the Commission rested its initial designation of Huawei on legal error, nonevidence and unreliable evidence, and irrational inference. *See supra* pp. 36-105.

[23] Unless the decisionmaker in the Bureau has been appointed by full Commission, rather than by Chairman Pai alone, any final designation would violate the Appointments Clause of the Constitution, U.S. Const. art. II, § 2, cl. 2. Because it involves a determination that an entity is a national security threat to the integrity of communications networks and the communications supply chain, Order ¶ 64, any final designation requires the exercise of "significant authority" under the laws of the United States. *See, e.g.*, *Lucia*, 138 S. Ct. at 2051. Consequently, the Constitution requires that the Bureau Chief and staff responsible for such determinations—all of whom hold "continuing" positions established by law, *see* 47 U.S.C. § 155(b), (c)(1); 47 C.F.R. §§ 0.191, 0.392—be "officers" appointed by the Commission as a whole pursuant to the Appointments Clause. *See Lucia*, 138 S. Ct. at 2051; *Free Enter. Fund*, 561 U.S. at 510-13. Because the Bureau Chief and staff are appointed not by the Commission but by the Chairman alone, their appointments do not conform with the Appointments Clause, and they may not constitutionally exercise the significant authority the Commission purported to delegate to them over the designation process. *See Free Enter. Fund*, 561 U.S. at 510.

The Commission relied on unsubstantiated speculation and assertion, as well as statutes, indictments, and unreliable congressional materials and "expert" reports. Compounding those legal errors, the Commission ignored Huawei's extensive evidence of its independence from the Chinese government and the safety and reliability of its products. The result was a determination, against the weight of the evidence, that Huawei somehow poses a national security threat to the integrity of communications networks or the communications supply chain.

The errors did not end there. The Commission also misconstrued Chinese law (thus infecting its designation decision with legal error) and failed to explain why other companies similar to Huawei should be treated differently (thus rendering its designation decision arbitrary and capricious). That was unsurprising, because, as the record shows, the Commission prejudged this case from the moment it decided to bow to congressional pressure.

For all these reasons, the Commission's initial designation of Huawei is legally invalid. And for that reason, the Bureau may not rely on it to support final designation. *See generally Chenery*, 318 U.S. at 87-90, 95.

2. Similarly, the Bureau may not make the same mistakes on which the Commission rested its initial designation—what was error for the Commission is error for the Bureau too

Just as the Bureau may not designate Huawei based on the Commission's invalid initial designation, the Bureau may not designate Huawei based on the same considerations that infected the Commission's initial designation. The Bureau may not repeat the Commission's legal errors by relying on speculative, unsupported assertions in statutes, indictments, congressional materials, and "expert" reports; ignoring Huawei's extensive evidence of its independence from the Chinese government and the safety and reliability of its products; misconstruing Chinese law; and failing

to explain why other companies similar to Huawei should be treated differently. A final designation that relies on these legal and factual errors would be just as legally invalid and arbitrary and capricious as the initial designation.

B. Additional evidence shows that designation of Huawei is improper

The Commission could not carry its burden of showing that designation of Huawei was warranted by a preponderance of the evidence. *See supra* pp. 36-105. The Bureau bears the same burden and cannot carry it either. Not only has the Bureau adduced no evidence, but Huawei now submits additional affirmative evidence reinforcing the impropriety of the designation and any final designation. *See infra* pp. 127-162. As insubstantial as the Commission's case was against Huawei, this additional evidence leaves no doubt that final designation would be improper and unsupported by a preponderance of the evidence. More specifically, this evidence reinforces the points that (1) Huawei is a private company that is independent from the Chinese government; (2) Huawei adheres to leading cybersecurity practices; (3) Huawei's customers (both civilian and government) have expressed satisfaction with the safety of its products; and (4) Huawei's entry into and presence in the U.S. market would improve, not threaten, market diversity and security.

1. Huawei is a private company that is independent from the Chinese government

Had the Commission given Huawei the required notice of its intent to designate Huawei—plus the standard on which it would base the designation, *see supra* pp. 2-4, 8-11, 25-27—Huawei would have had an opportunity to address the Commission's fundamental misunderstanding of the relationship between Huawei and the Chinese government. Contrary to the Commission's assertions, Huawei—a private company—does not have "close ties to the Chinese government," Order ¶ 48, and is not subject to "influence" from the Chinese government, nor from the Communist Party, Order ¶ 50. The Commission claims that "Huawei has refused to answer questions about its

ownership and governance," and thus "infer[s] that the Chinese government clearly has a vested interest in the company's success." Order ¶ 51 (citing the 2018 RWR Report). Of course, the Commission never posed such questions to Huawei, and Huawei was given no such chance to answer. Although it is impossible for Huawei to give a fulsome response given the Commission's lack of clarity, Huawei now submits additional evidence regarding (a) Huawei's independence from the Chinese government; (b) the background of Mr. Ren Zhengfei and his role in Huawei's corporate governance; (c) the role of the Communist Party Committee at Huawei; (d) the independence of Huawei's U.S. subsidiaries; and (e) the limited support Huawei receives from the Chinese government. This evidence confirms that the Chinese state has no influence over Huawei's business or activities, and it rebuts much of the Commission's stated basis for its designation.

a. Huawei is a private company that is not subject to Chinese government control

The Commission claims that "the Chinese government and the Chinese Communist Party … can exert influence over the corporate boards and management of private sector companies," but points to no evidence that Huawei's Board and management have been subject to such influence. Order ¶ 50. As described above, *supra* pp. 83-87, there was insufficient evidence before the Commission to establish that Huawei's leadership is controlled or influenced by the Chinese government.

Nonetheless, Huawei now submits additional evidence regarding Huawei's corporate governance and the independence of its boards of directors and rebutting the claims in the Order, including declarations from three senior executives—Alan Fan Zhiyong, Leon Wang, and Wei Jiang. Ex. C, Declaration of Alan Fanzhiyong ("Fanzhiyong Decl."); Ex. E, Declaration of Leon Wang ("Wang. Decl."); Ex. F, Declaration of Wei Jiang ("Jiang Decl.").

Mr. Ren Zhengfei founded Huawei in 1987 and became Huawei's CEO in 1988. Fanzhiyong Decl. ¶¶ 13, 15. The company was initially focused on selling equipment manufactured by other telecom companies and eventually began manufacturing telephone switches. *Id.* ¶¶ 13-14. Huawei grew slowly, gradually expanding its business over time, and investing heavily in research and development. The company has always been privately owned, and is now wholly owned by its employees and Mr. Ren.

Huawei Technologies and Huawei's three U.S. Operating Subsidiaries (Huawei USA, Huawei Device, and Futurewei) are all direct or indirect wholly owned subsidiaries of Huawei Holding. Wang Decl. ¶ 4; Fanzhiyong Decl. ¶ 16. Huawei Holding is a private company, owned entirely by employees (through Huawei's employee stock ownership plan) and Mr. Ren Zhengfei (as the only natural person shareholder). Wang Decl. ¶ 5; Fanzhiyong Decl. ¶ 16. No Chinese government or military entity holds any shares of Huawei Holding, Huawei Technologies, Huawei USA, Huawei Device, or Futurewei. Wang Decl. ¶ 15; Fanzhiyong Decl. ¶ 16. Each of the five Huawei entities described above has its own Board of Directors (in the case of Huawei Device USA, a single director). Wang Decl. ¶ 4.

Currently there are 17 individuals who serve as members of both the Huawei Holding and Huawei Technologies Boards of Directors ("Huawei Board Members"). *Id.* ¶ 8. All 17 Huawei Board Members are private citizens, and none holds positions in the Chinese government. *Id.* ¶¶ 8-9. Each Huawei Board Member has taken an oath agreeing not to receive any income from a source other than Huawei and not to take on outside employment, which includes employment in the Chinese government. *Id.* ¶ 10. Similarly, none of the individuals that serve as directors for Huawei USA, Huawei Device, or Futurewei holds any position in the Chinese government. *Id.* ¶ 14.

Huawei has previously explained that the company's business and investment decisions, research and development priorities, profit distributions, and staffing decisions are made and determined by the Board and are not controlled or influenced by the Chinese government, the Chinese military, or the CCP. *See supra* pp. 43-44 (citing 6/1/2018 Dowding Decl. ¶¶ 14-17; 8/6/2018 Huawei Ex Parte at 41-42). The additional evidence submitted by Huawei confirms this governance structure.

"Huawei's Charter of Corporate Governance ('Charter') and Huawei Holdings' Articles of Association ('Articles') empower Huawei's governance bodies, such as the Representatives' Commission (which exercises the rights and responsibilities of the employee shareholders) and the Board of Directors, to make decisions regarding major company matters." Fanzhiyong Decl. ¶ 17. Huawei's Board of Directors is responsible for "corporate strategy, operations management, ensuring customer satisfaction, and protecting shareholder interests." *Id*. ¶ 19. The Board of Directors and its Executive Committee are led by three rotating chairs, "who serves as the foremost leader of the company during his or her six-month term." *Id.* ¶ 20. Currently the rotating chairs are Mr. Xu Zhijun, Mr. Guo Ping, and Mr. Hu Houkun; none of the chairs holds any positions with the Chinese government or Huawei's Communist Party Organization. *Id.* ¶ 20; Wang Decl. ¶ 15.

Huawei does not provide special services to the Chinese government. Although Huawei's customers do include "local, provincial, and state government entities" in China, these sales only "accounted for around 2% of Huawei's revenue in 2018." Jiang Decl. ¶ 4. And under Huawei's corporate policy, all sales of products and services—including those to the Chinese government—are permitted only "for civilian end-use." *Id.* ¶ 5. However, as support for its argument that Huawei has an "established relationship with the Chinese government," the Commission adopted uncritically the HPSCI Report's statement that "Huawei provides special network services to an entity …

believe[d] to be an elite cyber-warfare unit within the PLA." Order ¶ 51 (citing HPSCI Report at 34). But this is not the case. Huawei submitted a statement to HPSCI that "Huawei has never done any customized R&D or production for the Chinese military or Chinese intelligence services" and that "Huawei has never managed any of the PLA's networks." 9/22/2012 Huawei Second Responses to HPSCI (Answer to HPSCI's Questions) at 12. Huawei's vigorous denials in 2012 were ignored in favor of an unsubstantiated rumor; a rumor the Commission simply adopted. In light of this sworn statement from Huawei now in the record here that Huawei did not, in fact, provide any such "special network services" to the PLA, and no evidence contradicting this statement, it would be impermissible for the Bureau to rely on the statement in the HPSCI Report as a basis for the designation.

There is simply no evidence in the record that the Chinese government has exerted any control or influence over Huawei's governance or leadership.

b. The service of Huawei's CEO, Mr. Ren Zhengfei, as a civil engineer in the Chinese army more than 30 years ago is not evidence of Chinese government influence

The Commission also argued that Mr. Ren's past military service and purported "ultimate veto authority" somehow make him subject to the influence of the Chinese government. Order ¶ 50. The Commission has nowhere explained why Mr. Ren's background in the military or Mr. Ren's role in Huawei's corporate governance is relevant to Huawei's designation, nor has the Commission pointed to any actual evidence that Mr. Ren has been subject to undue influence by the Chinese government. Although this lack of reasoned explanation makes it difficult to respond to the Commission, Huawei has submitted additional evidence to clarify both Mr. Ren's military service and his role in Huawei's corporate governance, neither of which justifies an inference that Mr. Ren has been influenced in any way by the Chinese government.

The Commission stated that "Huawei's founder, Ren Zhengfei, is himself believed to be a former director of the People's Liberation Army Information Engineering Academy, an organization associated with China's signals intelligence." Order ¶ 50 (citing HPSCI Report at 13-14). As described above, the Commission should never have relied on the unsubstantiated claims regarding Mr. Ren's background that were included in the HPSCI Report. *See supra* pp. 70-71. But in light of the additional evidence submitted by Huawei, there can be no mistake that Mr. Ren's military service did not involve signals intelligence in any way.

Mr. Ren studied architecture at the Chongqing Institute of Civil Engineering and Architecture and, following graduation, "was employed in the civil engineering industry until 1974." Fanzhiyong Decl. ¶ 4. In 1974, Mr. Ren joined the military as a technician in the Civil Engineering Corps. *Id*. After joining the military, Mr. Ren was assigned to Liaoyang to assist in building a synthetic fiber factory for clothing production. *Id.* ¶ 5; *see also* Ex. OO, Gei Tai, Civil Engineering Corps, Ren Zhengfei (Oct. 18, 1978) ("Gei Tai, Civil Engeineering Corps, Ren Zhengfei").

While working on this project, Mr. Ren developed a novel instrument akin to a pressure gauge for use in the clothing factory. Fanzhiyong Decl. ¶¶ 6-7; Ex. PP, Wenhui Bao, China's first high-precision measuring quasi-equipment, Oct. 14, 1977; Gei Tai, Civil Engeineering Corps, Ren Zhengfei. After he developed the instrument, Mr. Ren was promoted to engineer. *Id.* ¶ 8; Gei Tai, Civil Engeineering Corps, Ren Zhengfei. Mr. Ren later received a promotion to Deputy Director (a position with no military rank) of a small construction research institute with just over twenty employees. Fanzhiyong Decl. ¶ 9. This was the highest position Mr. Ren achieved during his time with the military. *Id.* Mr. Ren retired from the army when China disbanded the entire Engineering Corps in 1983. *Id.* ¶ 10.

Mr. Ren never worked at the People's Liberation Army Information Engineering Academy, nor did he ever serve as Director or Deputy Director of that Academy. *Id.* ¶ 11. In addition, "Mr. Ren's military service did not involve Chinese signals intelligence in any way." *Id.* Mr. Ren was merely a civilian engineer in the military akin to a civilian employee of the U.S. Army Corps of Engineers; he served for just nine years; and he was never a high-ranking member of the military. As explained above, the Commission's "evidence" to the contrary on this point consists of nothing more than unsubstantiated assertions that any rational decisionmaker would be required to disregard.

The Commission's depiction of Mr. Ren's "veto authority" is similarly unfounded. In support for its assertion that Mr. Ren has "ultimate veto authority," the Commission cites only to the 2018 RWR Report, which, perhaps unsurprisingly contains no support for its mischaracterization. Order ¶ 50 (citing 2018 RWR Report at 13). Huawei's corporate governance articles contradict the RWR Report's (and the Commission's) depiction of Mr. Ren's role in Huawei's corporate governance.

Huawei's governance bodies, including the Representatives' Commission and the Board of Directors, make decisions based on majority rule, and each member (including Mr. Ren) has only one vote. Fanzhiyong Decl. ¶¶ 17-18. Huawei's Charter provides Mr. Ren with certain limited and specifically defined veto powers, including the right to veto amendments to governance documents or to veto increases or decreases in the registered capital of Huawei. *Id.* ¶ 21. Mr. Ren's veto authority, however, does not empower him to exercise unilateral control over Huawei, and he does not have an absolute right to veto any company matter. *Id.* ¶¶ 21-22. For example, Mr. Ren

"does not have the power to veto business decisions or financial plans that do not change the company's nature, corporate form, or shareholder structure." *Id.* ¶ 22. And in practice, Mr. Ren has never exercised his veto power. *Id.* ¶ 23.

In light of this additional evidence, it would be irrational for the Bureau to make the same mistake as the Commission by relying on incorrect and unsourced assumptions about Mr. Ren's background and business authority.

c. Huawei, like other private companies in China, has a Communist Party organization, but that organization has no management or governance role

As support for its claim of close ties, the Commission pointed out that "the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions." Order ¶ 50 (citing HPSCI Report at 23). But it is unremarkable that Huawei maintains a Party organization, because it is required to do so by Chinese law, and Party organizations are quite common in China (including among U.S. companies). Given that the vast majority of foreign and domestic companies that operate in China have such an organization, it is illogical that Huawei's Party organization should serve as evidence that the company has some untoward connection with the Communist Party or serve as a basis to single Huawei out for designation. *See ACA Int'l* v. *FCC*, 885 F.3d 687, 697-700 (D.C. Cir. 2018) (holding that the FCC could not reasonably conclude that every cell phone is an "automatic telephone dialing system" for purposes of the Telephone Consumer Protection Act because then "every smartphone user violates federal law whenever she makes a call or sends a text message without advance consent"). To clarify the role of Party organizations in China and Huawei's Party organization, Huawei submits the Wang declaration, as well as an expert report from Professor Randall Peerenboom, who is an expert in Chinese law and has significant experience with corporate governance and the role of party committees in China. Ex. G, Expert Report of Randall

Peerenboom ("Peerenboom Report"). These materials explain that Party organizations in private companies do not have the influential role the Commission ascribed to them.

As Professor Peerenboom explains in the attached expert report, "[a]rticle 30 of the Constitution of the Communist Party of China ('CCP Constitution') requires the formation of a Party organization in all companies with three or more Party members." Peerenboom Report ¶ 27. This requirement applies to all state-owned entities, domestic private companies such as Huawei, and foreign invested enterprises, including joint ventures and wholly foreign-owned enterprises. *Id.* (citing CCP Constitution art. 30). And "Article 19 of the Company Law of the People's Republic of China requires companies to provide the 'necessary conditions' for the activities of Party organizations, which shall be established within the company according to the CCP Constitution." *Id.* ¶ 28 (citing Company Law of the People's Republic of China (rev. 2018), 2018 China Law LEXIS 1317).

Professor Peerenboom explains that "[t]he CCP Constitution and other Party regulations distinguish between the role of the Party organizations in state-owned entities and in private companies, like Huawei," with Party organizations playing a decidedly more minor role in private companies.[24] *Id.* ¶ 29. For example, Article 33 of the CCP Constitution calls on Party committees within state-owned enterprises to assume a leadership role in deciding major issues for the company. *Id.* "In sharp contrast, Article 33 contemplates a *much more circumscribed role* for party organizations *within private companies*." *Id.* ¶ 30. As described above, *see supra* pp. 43-44, 84, the Party organizations are charged primarily "with ensuring the company complies with generally

[24] *See also supra* pp. 100-01 (general discussion of Chinese law requirements for party committees). Although PRC regulations refer to, and sometimes distinguish among, the party organization and the party committee, "in practice the terms are used interchangeably," and "nothing substantive hinges on the difference in terms" for the purposes of these comments. Peerenboom Report ¶ 12 n.2.

applicable laws, overseeing the trade union, and promoting the healthy development of the company. They are notably not given a role in the daily operation of the company or in deciding major issues." *Id.* (emphasis omitted). Similarly, Article 10 of the Party Branch Work Regulations explicitly contemplates a distinction between Party committees at state-owned enterprises and non-state-owned enterprises. *Id.* ¶¶ 31-33. The Party committee in state-owned enterprises should "focus their work on the operations of their enterprise, [and] discuss and decide on major issues of the enterprise in accordance with regulations." *Id.* ¶ 32 (quoting Article 10(3) of the Party Branch Work Regulations) (emphasis omitted). Whereas the Party organization in a "non-public economic institution" "provides guidance to and oversees the enterprise in strictly observing the laws and regulations of the state, unites the workers and the masses, upholds the rights and interests of all parties according to law, establishes a modern corporate culture and promotes the healthy development of the enterprise." *Id.* ¶ 33 (quoting Article 10(5) of the Party Branch Work Regulations). The regulations simply do not require Party organizations in private companies to carry out the Party's principles or policies" or play any other leadership role. *Id.* The Commission's misunderstanding of the requirements that Chinese law imposes on the interaction between a company and its Party organization in a private company vis-à-vis a state-owned company leads it to make assumptions that are unfounded in law or fact.

Given the legal requirement that Party organizations be established in companies with three or more Party members, Party organizations are common in all types of entities operating in China, whether state-owned enterprises, Chinese private companies, or foreign-invested enterprises. *See id*. ¶ 11. Professor Peerenboom finds that over 99.98% of state-owned enterprises have a Party committee, while about 68% of domestic private companies and 70% of foreign invested enterprises have Party organizations. *Id.* ¶ 37. Other telecommunications and technology companies,

including some of Huawei's competitors, have Party committees. *Id.* ¶¶ 38-39 (Nokia, Samsung, Toshiba, Tencent, Xiaomi, Sina, and Baidu all have Party committees). Even U.S. companies that operate in China have Party organizations. *Id.* ¶ 40 (Walmart, General Electric, Walt Disney, Dupont, and Deloitte all have Party committees). "It is unremarkable, therefore, that Huawei, like the vast majority of other domestic and foreign companies that operate in China, has a party organization … in compliance with Chinese law." *Id.* ¶ 13.

Professor Peerenboom concludes that "the available evidence shows that party organizations play a circumscribed and benign role in both private domestic and foreign companies, and that they do not generally participate in daily operations or in making major business decisions." *Id.* ¶ 42. The "evidence confirms the prescribed role of party organizations in private companies under PRC law, which as discussed above, is far more limited than that of [state-owned entities]." *Id.* ¶ 43. One Party member at a U.S.-based Fortune 500 company described the Party committee as engaging in activities like planting trees, sponsoring outings to go see movies, and providing summaries of the CCP State Council meeting. *Id.* ¶ 44 & n.75 (describing a media interview with Walmart's Tianjin store Party committee secretary who said most members of Walmart's Party organization are midlevel or senior executives who study Party materials and noting that other analysts said Party organization branches in other multinational companies generally do not interfere with company management). Party organizations have also been described as "auxiliary human-resource departments" that help advise company managers on government policies, help recruit and cultivate talent, and resolve friction between management and employees. *Id.* ¶ 48.

In compliance with Chinese law, Huawei has a Party organization ("Huawei Party Organization") that serves Party members employed by Huawei in China. Wang Decl. ¶ 7. But no Huawei Board Member holds any leadership position in the Huawei Party Organization, nor does

any member of the Huawei USA, Huawei Device USA, or Futurewei Board of Directors. Wang Decl. ¶¶ 9, 14. Further, Huawei's corporate governance documents include a detailed description of the allocation of power and the decisionmaking authority for daily operation and major business decisions, but do not assign the Huawei Party Organization any role in daily business operations or in making major commercial decisions. Peerenboom Report ¶ 53; Fanzhiyong Decl. ¶¶ 17, 19-20.

Consistent with the media descriptions regarding Party organizations in private companies, the role of the Huawei Party Organization has been described as "educating employees and increasing employee awareness" and "remind[ing] staff to comply with regulations and obey the law, to help ensure internal and external compliance." Peerenboom Report ¶ 24 (citing In His Own Words, Dialogues with Ren Vol. I (Exhibit D), at 86-87 (Japanese Media Roundtable)). Mr. Ren has also repeatedly explained the limited role of the Party organization at Huawei, emphasizing that "the Party organization is not integrated into the governance structure and does not participate in any business management or business decisionmaking." *Id*. ¶ 55 & n.95 (collecting citations). He has unmistakably stated: "Huawei's party committee isn't in any way involved in our business decisions." In His Own Words, Dialogues with Ren Vol. I (Exhibit D), at 297.

The structure and operation of the Party organization in Huawei stands in stark contrast to the Party committees in state-owned or public enterprises. For example, in Nokia Shanghai Bell, the chairman of the board of directors also serves as the secretary of the company's Party committee. Peerenboom Report ¶ 39. By contrast, none of Huawei's board of directors serves in a leadership role in the Party organization. *Id.* ¶ 57; Wang Decl. ¶¶ 9, 14; *see also* Ex. M, Ex. 71 to Huawei Motion for Summary Judgment, *Huawei Technologies USA, Inc., et al.* v. *United States*, No. 4:19-cv-00159 (E.D. Tex.) (showing the role of the Party committee in Nokia Shanghai Bell).

Professor Peerenboom concludes that "Mr. Ren's description of the Huawei Party Organization serving in a limited role is consistent with academic articles, empirical surveys, media reports, my own experience and understanding of the circumstances, and PRC law." Peerenboom Report ¶ 58. He finds "no indication that the Chinese government could or would exert influence over major corporate decisions or the daily operations of the company through the Huawei Party Organization." *Id.* ¶ 61.

Given that Party organizations are a routine part of business in China, and that there is no evidence that the Party organization plays any role in Huawei's corporate governance, there is no basis for concluding that the existence of a Party organization is evidence of control or undue influence by the Chinese government, or that it somehow otherwise justifies Huawei's designation.

d. The little government support that Huawei receives does not evidence undue influence in any way

The Commission appeared to believe that Huawei is "being financed by the Chinese government," Order ¶ 6, and that Huawei "is treated as a state-owned enterprise and has benefited from state procurement funds, subsidized financing from state-owned policy banks and state funding for research," Order ¶ 51; *see also id.* ¶ 30 (asserting that Huawei is the recipient of "favorable subsidies and other benefits bestowed by governments that are in an adversarial position to the United States"). But the Commission failed to support these claims with any actual evidence, or to explain how the receipt of government support correlates to security risk. *See supra* pp. 84-85, 110-12. Huawei nonetheless submits further evidence to clarify that the level of support that it receives from the Chinese government is immaterial to its cost structure and financial performance; that such support is consistent with the types and level of support provided to Huawei's competitors by their respective governments; and that no evidence indicates that such support confers a competitive advantage to Huawei. This evidence includes an expert report from Professor Wei

Jiang, a Professor at Columbia University's Graduate School of Business, and an expert in corporate finance, corporate governance and institutional investors. Jiang Report.

As an initial matter, Professor Jiang finds that the Commission's assertions about the amount of support Huawei allegedly receives are largely unsupported by empirical evidence or analysis. Jiang Report ¶¶ 15-22; *see also supra* pp. 84-85. The sources to which the FCC points generally provide no data or other evidence on the amount of support Huawei supposedly receives. *See* Jiang Report ¶¶ 15-22. And even in the few cases in which a data point is provided, the FCC points to no evidence demonstrating that the support Huawei receives is provided on terms more favorable than Huawei could have obtained from commercial sources. *Id.* ¶ 17. Further, as Professor Jiang explains, in order to determine whether government support provides Huawei with a competitive advantage, "one must assess the level and terms of support that Huawei has received *relative to Huawei's competitors*. The FCC, however, fails to provide any such analysis, making it impossible to assess whether Huawei has benefited from lower costs." *Id.* ¶ 18 (emphasis added).

Professor Jiang then engages in the empirical analysis that the Commission failed to do. Upon a close reading of the FCC's Order and the various documents cited in the FCC's Order, she identifies four categories of support allegedly provided to Huawei by the Chinese government: government grants; bank loans with favorable interest rates; and government-sponsored export credit for overseas customers; and preferential tax treatment. *Id*. ¶ 16. But, as she explains, for each category, any support is immaterial, provided on terms similar to those available commercially, and/or comparable to that received by other companies, including Huawei's competitors.

First, Huawei receives grants from the Chinese government, but such support is "not material to Huawei's cost structure and financial performance." Jiang Report ¶ 37. For example, for

each year between 2009 and 2018, the removal of such support would have resulted in a 0.6% or lower change in revenue, as well as only a small change in operating profit. *Id.* & Ex. 3. Further, government grants to support activities such as research and development are common practice in many countries. *Id.* ¶ 36. Other companies in other countries, including Huawei's competitors such as Ericsson in Sweden and Nokia in Finland, also often receive government grants. *Id.* ¶ 35 & Ex. 2.

Second, the Commission also seemed to claim that Huawei has benefitted from state-owned banks. Order ¶ 51 (referencing "subsidized financing from state-owned policy banks"). But as of 2018, the large majority of Huawei's debt—75%—came from institutions and markets outside of China. Jiang Report ¶ 45. Moreover, Huawei does not receive more favorable interest rates relative to market interest rates for either its USD- or CNY-denominated debt. *Id.* ¶¶ 46-47 & tbls.6-7. In fact, over the 10-year period from 2009 to 2018, Huawei's effective interest rate was *higher* than that of Cisco, Ericsson, and Nokia. *Id.* ¶ 50. Further, unlike its competitors, Huawei has shown itself to be capable of self-financing its growth by using cash flows generated from operations without the need for external financing. *Id.* ¶ 48. Thus, any state-owned bank loan that Huawei did receive would not be material to its ability to meet its investment needs or its financial performance. *Id.*

Lastly, the Commission took issue with Huawei-related projects funded by the Exim Bank of China, the China Construction Bank, and the China Development Bank. Order ¶ 51. But the Commission appeared to misunderstand the nature of export credits. That is not surprising, because the Commission cannot claim to have any expertise in the areas of international export credits and financing. These financing facilities each "provide[] support for exported goods and services by offering credit to creditworthy foreign borrowers to make their purchase." Jiang Report ¶ 52. The

loans are provided directly to the foreign customer, and not to Huawei. *Id.* These loans are the result of negotiations between the foreign customer and the commercial bank. *Id.* The government-sponsored credit lines that Huawei's customers have access to do not provide an unfair advantage vis-à-vis credit lines available to customers of its competitors. *Id.* ¶ 53. Indeed, both the Swedish Export Credit Corporation, a government-owned agency whose business is "to lend money to Swedish export companies and their buyers abroad," and Finnvera, a specialized financing company owned by the State of Finland, that "strengthens the operating potential and competitiveness of Finnish enterprises by offering loans, domestic guarantees, export credit guarantees and other services associated with the financing of exports," provide similar credits to customers of Ericsson and Nokia. *Id.* ¶ 51. Ex. TT, Finnvera, Buyer financing arranged through cooperation between export credit agencies (Sept. 10, 2017). As a result, "there is no indication that these credit lines accessible to Huawei's customers provide Huawei an unfair competitive advantage relative to its peers, and the FCC provides no evidence in support of such a claim." *Id.* ¶ 53.[25]

e. The Bureau has no basis for designating Huawei's affiliates, including Huawei USA

Once again, the Commission provided no factual or legal support for its conclusion that "equipment from subsidiaries, parents, and affiliates pose the same risks to network integrity as

[25] The sources on which the Commission relied also claim that Huawei is the recipient of allegedly preferential tax treatment. But, as with many countries, China's tax laws provide for lower rates or tax breaks for companies meeting prescribed criteria. Jiang Report ¶ 38. Thus, for example, Chinese law provides for a lower rate for "High and New Technology Enterprises" for any company meeting certain criteria, and Huawei uses such tax treatment where it qualifies, as do other companies in China, including those that are foreign-owned. *Id.* ¶¶ 38-41. Such tax policies are common tools for governments to incentivize the development of certain industries and to foster research and development. *Id.* ¶ 42. Indeed, while Huawei's effective tax rate fluctuated around 10% below the statutory tax rates between 2009 and 2018, the effective tax rate for corporations in the United States was approximately 19% below the statutory rate in the ten years prior to 2018. *Id.* ¶ 43.

equipment directly from the covered company," nor did the Commission demonstrate that any Huawei USA (or any other affiliate) has material ties to the Chinese government by virtue of its corporate relationship with Huawei Technologies. Order ¶ 39. Instead, the Commission based its designation of Huawei's affiliates on a vague concern that the Chinese government might "exert" influence over Huawei's affiliates. Order ¶ 56 & n.178. As stated above, there is no evidence in the record that demonstrates any relationship between Huawei's U.S. Operating Subsidiaries and the Chinese government.

Nonetheless, Huawei now submits additional evidence to refute any suggestion of a connection between these entities and the Chinese government and to make clear that Huawei's U.S. Operating Subsidiaries are U.S. corporations that are bound by, and seek to comply with, U.S. laws. This evidence includes: (1) a supplemental declaration from Thomas Dowding ¶ 1 ("2/3/2020 Dowding Decl."); (2) a declaration from Timothy Danks, who has served as the Vice President of Risk Management and Partner Relations for Huawei USA since 2019 and has thirty years of experience in the telecommunications industry (Declaration of Timothy Danks ¶¶ 1, 6 ("Danks Decl.")); (3) an affidavit from David He, who has over twenty years of business experience in the telecommunications industry and serves as the President of Huawei USA (Ex. L, Affidavit of David He ¶¶ 1, 11, *Huawei Technologies USA, Inc., et al.* v. *United States*, No. 4:19-cv-00159 (E.D. Tex.) ("He Aff.")); (4) an affidavit from Li Xu, who serves as the Team Leader of the Corporate Law Legal Team in the Legal Department of Huawei Technologies (Ex. UU, Affidavit of Li Xu ¶ 1, *Huawei Technologies USA, Inc., et al.* v. *United States*, No. 4:19-cv-00159 (E.D. Tex.) ("Xu Aff.")).

As described above, Huawei has three Operating Subsidiaries in the United States: Huawei USA, Huawei Device USA, and Futurewei. Wang Decl. ¶ 3. Each of these entities is a U.S. corporation organized under the laws of the State of Texas; has its own board of directors (or, in Huawei Device USA's case, director); and has its own officers and employees. Wang Decl. ¶¶ 11-13; He Aff. ¶ 5. No member of the Huawei USA or Futurewei Board of Directors, or the director of Huawei Device USA, holds any position in the Chinese government or Huawei Party Organization. Wang Decl. ¶ 14; Xu Aff. ¶ 9. Huawei USA, Huawei Device USA, and Futurewei are all wholly owned direct or indirect subsidiaries of Huawei Holding and have no Chinese government ownership. Wang Decl. ¶ 15; Xu Aff. ¶¶ 4-5, 10. All three entities operate independently of the Chinese government. Wang Decl. ¶ 15; Xu Aff. ¶ 10.

Within the United States, Huawei Device USA sells only limited products, such as "handsets and other consumer devices," and Futurewei "handles [only] research and development." 2/3/2020 Dowding Decl. ¶ 11 n.2. Neither "sell[s] telecommunications infrastructure product or services in the United States to carrier customers." *Id.* Therefore, the Commission's sweeping and utterly unnecessary designation lacks any rational application to these entities.

More specifically, Huawei USA "is the only Huawei-affiliated entity authorized to sell telecommunications infrastructure products and services to carriers in the United States." *Id.* ¶ 11; *see also* Danks Decl. ¶¶ 9-10; He Aff. ¶ 4. The Commission's blanket designation failed to consider the nature of Huawei USA's business or the extensive insulating measures inherent in Huawei USA's products and services. Indeed, Huawei USA "does not operate or manage any telecommunications networks" and "does not provide managed services to any customers in the United States." 2/3/2020 Dowding Decl. ¶ 24; Danks Decl. ¶ 11. Moreover, Huawei USA "does not have direct or unmonitored access to its customers' networks and/or data." 2/3/2020 Dowding

Decl. ¶ 29; *see also id.* ¶ 28, 30-31; *id*. ¶ 27 ("Huawei Technologies USA does not provide any services that involve storing end user data of its carrier customers … that would give [it] or any of its affiliates unmonitored access to its customers' network information."); Danks Decl. ¶¶ 16-20; *id*. ¶¶ 21-25 (explaining that "[a]ll customer network access [goes] through the SNAS," which "only permits remote access from within the U.S.," and which is isolated from Huawei USA's internal corporate network by "a perimeter network dual firewall"). Contrary to the Commission's fearmongering, Huawei USA's products and services simply do not present the security risks that the Commission's designation seeks to mitigate.

Further, Huawei USA has its own financial statements and plans, as well as its own employees—226 employees as of April 30, 2019. He Aff. ¶ 5. As of that same date, "approximately 90% of these employees were U.S. citizens or permanent residents who were hired directly by Huawei USA, rather than individuals hired by Huawei Technologies in China who were living and working temporarily in the United States." *Id.* ¶ 5. The Commission certainly has no basis to conclude that U.S. citizens and residents would assist in sabotaging their own telecommunications networks. As Timothy Danks explained, "I have called the United States home for almost twenty years, raised a family here and would never take any action that would betray the United States or compromise my status and eventual citizenship here. Nor has Huawei ever asked me to take any action to do so." Danks Decl. ¶ 5.

The Commission noted, but did not refute, Huawei's statement that "its foreign affiliates are not beholden to Chinese law." Order ¶ 56 n.178. To be clear, as the President of Huawei USA, David He, explains: "Huawei USA is a corporation organized under Texas law [that] markets and sells products exclusively in the United States, and, in doing so, is bound to comply with, and seeks to comply with, the laws of the United States." He Aff. ¶ 5; *see also* Danks Decl. ¶ 33

("Huawei Technologies USA abides by all local laws and regulations with respect to data and privacy"). He confirms that "[b]ecause Huawei USA is legally separate from and in these respects operates independently of Huawei Technologies, Huawei USA's legal obligations are distinct and independent of the legal obligations of Huawei Technologies." He Aff. ¶ 5.

There continues to be no evidence in the record of any link whatsoever between Huawei's U.S. operating subsidiaries and the Chinese government. Given the additional evidence now submitted by Huawei, the Commission's previous vague concerns on this point cannot serve as the basis for any designation by the Bureau.

2. Huawei is a leader in deploying robust cybersecurity practices and does not collect customer data or manage their networks

Huawei now submits additional affirmative evidence further detailing its rigorous cybersecurity measures. More specifically, Huawei USA has submitted sworn statements detailing its commitment to abiding by all local laws and regulations with respect to data and privacy, including the laws of the United States. *See* Danks Decl. ¶ 33. Further, as Timothy Danks, who manages cybersecurity and privacy risks, explains, Huawei USA follows strict cybersecurity policies to which all employees and contractors must conform. *See, e.g*, *id*. ¶¶ 26-30. Among other things, Huawei USA implements training programs and security protocols that ensure the prompt detection and reporting of any security incidents. *See id.* ¶¶ 28-29. Additionally, the company regularly performs audits to ensure compliance with its cybersecurity policies. *See id.* ¶ 30.

Despite the Commission's suggestion to the contrary, there is no evidence in the record that rebuts these statements. Although the Commission points to reports by Finite State and the UK HCSEC, neither report comes close to establishing that Huawei presents a security risk. *See supra* pp. 79, 88. And Huawei now submits further evidence of its position as an industry leader in implementing robust cybersecurity standards and of its products' record of exceeding industry

standards in categories like security governance, security design, security testing, and secure coding. *See, e.g.*, Ex. RR, Huawei, *Huawei Completes BSIMM Assessment of its Industry-Leading Software Security Capabilities* (June 8, 2018). In 2013, Huawei invited Cigital, an independent U.S. third-party company (now part of Synopsys) to conduct a Building Security in Maturity Model ("BSIMM") assessment on the software security engineering capabilities for Huawei's products; Huawei has undergone multiple rounds of assessment from 2013 through 2018. *Id.* Moreover, Huawei's products ranked among the highest across more than 100 ICT companies and other enterprises in the BSIMM data pool. *Id*. Huawei has always been committed to the highest standards in cybersecurity, requiring continuous risk assessment and optimization. *See, e.g.*, 2018 Huawei Annual Report (announcing an initial budget of $2 billion USD for a "companywide transformation aimed at enhancing … software engineering capabilities").

Moreover, contrary to the Commission's allegation that Huawei "possess[es]" "a nearly unimaginable amount of data," Order ¶ 56 (citing Priscilla Moriuchi, *The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture*, Recorded Future (June 10, 2019) ("Recorded Future Report"), Huawei USA does not collect, store, or have direct or unmonitored access to any of its customer's networks and data, *see, e.g.*, 2/3/2020 Dowding Decl. ¶¶ 29-31. Rather, the company's "customers control all collection of, access to, and security of, their end users' data." Danks Decl. ¶ 12; *see also id.* ¶¶ 31-41. In the rare instances in which Huawei USA does receive access to customer data, it does so with prior customer approval, and the type of data accessed is strictly diagnostic and devoid of any personally identifiable information ("PII") of end-users or communications content–related information. *See id.* ¶¶ 15-20. All such diagnostic data is access-regulated and destroyed pursuant to data retention policies. *See id*. ¶ 43. Moreover, such access is permitted only through SNAS, a process that logs and records any instance of remote

access, providing customers with "a fully auditable record of every interaction with the customer's network." *Id.* ¶¶ 14-15, 25; *see also supra* pp. 48-49. The SNAS prevents any potential access from China, and permits authorized access originating only from within the United States. *See id.* ¶ 21. Huawei USA's network is also independent of, and isolated by a dual firewall from, the SNAS and network diagnostic data. *See id.* ¶ 24.

Because Huawei has only limited and monitored access to diagnostic data—and no access to PII or communications content—there is no basis for the Commission's assertion that Huawei's access to data "combined with its close ties to the Chinese government and its obligation under Chinese law to assist with Chinese intelligence-gathering mean that 'Huawei is potentially subjected to a government-driven obligation to capitalize on its global network and consumer devices ecosystem to fulfill core [Chinese government] national security and economic dominance objectives.'" Order ¶ 56 & n.176 (quoting Recorded Future Report at 15). As even one of the media articles cited by the Recorded Future Report itself concluded, "no evidence [exists] that Huawei's telecoms network equipment was ever used by the Chinese government—or anyone else—to gain access to the data of their customers." Karishma Vaswani, *Huawei: The Story of a Controversial Company*, BBC (Mar. 6, 2019)); *see* Recorded Future Report at 9. "Speculation is, of course, no substitute for evidence," *White ex rel. Smith*, 167 F.3d at 375, and "unsupported assertion[s]" are not reliable, *Safe Extensions*, 509 F.3d at 605. And the report's "bottom line" conclusion—both tentative and baseless—that Huawei is potentially subjected to the governmental objectives "supplies nothing of value" as an evidentiary matter. *Mid-State Fertilizer Co.*, 877 F.2d at 1339.

Finally, the Commission also alleged that Huawei poses a security risk because it "offers services managing telecommunications equipment." Order ¶ 45. But here again, the Commission's claim founders on the actual facts. As Dowding explains, Huawei USA does not manage or operate

any telecommunications networks, and it does not provide managed services to any carrier in the United States. *See* 2/3/2020 Dowding Decl. ¶ 24. Nor do the products that Huawei USA sells enable or require Huawei to manage or operate customer networks. Indeed, Huawei USA's management software does not provide it with any capability for managing customers' networks, and its technical services solutions are independently installed by customers, likewise without the company's access to customer networks. *See id.* ¶¶ 25-26. Huawei USA's "customers own the equipment and operate and manage the networks without operational assistance from" the company. *See id.* ¶ 20. Further, Huawei does not provide automated patching of these networks. Instead, updates and upgrades are tested by independent laboratories and installed by customers. In the limited instances in which Huawei USA does assist in software upgrades or installation services, all network access is authorized and can be monitored and audited by customers using the SNAS. *See id.* ¶¶ 21-26.

3. Huawei's customers (both civilian and government) have expressed satisfaction with the safety of its products

Huawei already has submitted evidence demonstrating its long history of strong customer satisfaction in the international arena, leading many countries to reject company-specific bans for their 5G networks. *See supra* pp. 51-54. To support its proposed designation of Huawei, the Commission purported to rely on "similar assessments by other countries" to exclude Huawei from 5G deployment. Order ¶ 53. To begin with, the Commission's focus on decisions made by other countries with respect to their 5G networks was misplaced. The Commission's rule applies well beyond 5G, and the equipment that Huawei supplies in the U.S. is, at present, *exclusively* 4G or older generations of technology. 2/3/2020 Dowding Decl. ¶ 16. Thus, to the extent the Commission relied on accurate facts, its reasoning still fails to support excluding Huawei from the entirety of U.S.

telecommunications networks, much less designating Huawei as a national security threat to the integrity of communications networks and the communications supply chain.

More importantly, the Commission both cherry-picked the other nations' assessments that it chose to reference and ignored the circularity of citing determinations that came about only through express U.S. government pressure. More specifically, the Commission cited actions by Japan, Australia, and New Zealand as support for its designation, but those newspaper articles, with their vague references to "security threats," do not show that any of those countries' decisions were made independently or were based on independent security risk assessments. Moreover, the Commission's reliance on newspaper articles that vaguely reference "security threats" does not show that any of those countries independently evaluated any security threat posed by Huawei or that the Commission even attempted to verify that the countries performed independent evaluations. Order ¶ 53 nn.163, 164, 165. Instead, most of the articles point out that the U.S. Government has exerted and continues to exert substantial pressure on its allies to ensure the very same outcomes it aims to achieve with this proposed designation. *See, e.g.*, Ex. FF at 1-4, Sam Sachdeva, *U.S. Delivers Five Eyes Threat over Huawei*, Newsroom New Zealand (Feb 22, 2019) ("The United States has delivered the most explicit threat yet to New Zealand's role in the Five Eyes alliance if it allows Huawei into the 5G network, saying it will not share information with any country which allows the Chinese company into 'critical information systems.'"). In essence, in an attempt to imply that its proposed designation is supported on an international scale, the Commission now pointed to measures which came about as a direct result of U.S. government coercion. *Cf. supra* pp. 53-54.

In so doing, the Commission inexplicably continued to ignore the *far greater* number of countries, including U.S. allies, who have resisted U.S. pressures to exclude Huawei from their 5G

networks. For example, the UK government announced last week that it will not ban Huawei equipment from its 5G networks in spite of "intense lobbying" by the Trump Administration. *See* Ex. FF at 5-7, Adam Satariano, *Britain Defies Trump Plea to Ban Huawei From 5G Network,* N.Y. Times (Jan. 28, 2020) ("Britain said on Tuesday that it would not ban equipment made by the Chinese technology giant Huawei from being used in its new high-speed 5G wireless network, the starkest sign yet that an American campaign against the telecommunications company is faltering."). Recent comments by the UK's Scientific and Technology Committee ("UK-ST Committee") reinforce Huawei's viability as a secure provider for telecommunications equipment. In testimony before the House of Commons UK-ST Committee, Professor Rahim Tafazolli, from the University of Surrey, was asked whether the UK needed to exclude Huawei equipment out of national security concerns. *See* Ex. FF at 8-61, Transcript, Q21, *Oral Evidence: UK Telecommunications Infrastructure, HC 2200,* Science and Technology Committee, House of Commons London (June 10, 2019). Because customers—not Huawei—manage networks and interact with user data, Professor Tafazolli explained that customers shoulder the burden for network security. *See id.* ("[T]hey have to make sure that each node as well as the whole network is secure and operated securely."). And the UK-ST Committee chairman concluded that there were "no technical grounds for excluding Huawei entirely from the UK's 5G or other telecommunications networks," and that "the potential benefits of 5G are clear" and the removal of Huawei from the current or future networks could cause significant delays. *See* Ex. FF at 62-69, Letter, Rt Hon. Norman Lamb, MP, Chair *Telecoms Supply Chain Review*, Science and Technology Committee, House of Commons London (July 10, 2019), https://www.parliament.uk/documents/commons-committees/science-technology/Correspondence/19-07-10-Chair-to-SoS-DCMS-re-the-Telecoms-Supply-Chain-Review.pdf.

Other European countries have declined to impose a ban as well, including France, Hungary, the Netherlands, Portugal, and Poland. Ex. FF at 70-71, *France Will Not Exclude China's Huawei from 5G Rollout: Minister*, Reuters (Nov. 25, 2019); Ex. FF at 72-75, *Hungarian Minister Opens Door to Huawei for 5G Network Rollout*, Reuters (Nov. 5, 2019); Ex. FF at 76-77, *No Huawei Ban in Dutch 5G Rollout: Government*, Reuters (July 1, 2019); Ex. FF at 78-80, Barry Hatton and Kelvin Chan, *Portugal Resists US Appeal to Bar Huawei from 5G Network*, AP News (Dec. 5, 2019); Ex. FF at 81-82, *Polish Govt Won't Exclude Huawei from 5G Deployment*, Telecompaper (Sep. 23, 2019). In fact, the European Union has adopted guidelines for member states to mitigate 5G security risks and, in doing so, affirmatively declined to enact a company-specific ban. Ex. FF at 140-42, Helene Foquet and Natalia Drozdiak, *EU Won't Recommend Banning Huawei in Upcoming 5G Risk Rules*, Bloomberg News (Jan. 20, 2020); *see also* Ex. FF at 143-44, Matina Stevis-Gridneff, *EU Recommends Limiting, but Not Banning, Huawei in 5G Rollout*, New York Times (Jan. 29 2020).

In addition, Norwegian Minister of Digitalization Nikolai Astrup confirmed that Norway has no plans to block Huawei from participating in 5G deployment. Ex. FF at 83-85, David Nikel, *Norway Open to Huawei Supplying 5G Equipment*, Forbes (Sep. 30, 2019). German officials have publicly and repeatedly defended the government's decision not to impose a ban on Huawei, commenting that Germany would have difficulty deploying 5G without Huawei participation. Ex. FF at 86-88, Patrick Donahue and Stefan Nicola, *Trump Germany Envoy Calls U.S.-China Spying Comparison Insulting*, Bloomberg News (Nov. 25, 2019) (Economy Minister Peter Altmaier noted that "[t]he U.S. also demands from its companies that they pass on certain information that are needed to fight terrorism."); Ex. FF at 145-47, Polina Strelnikova, *Germany Can't Set Up 5G*

Network Without China's Huawei, Interior Minister Says, Sputnik News (Jan. 18, 2020), ("Germany's Interior Minister Horst Seehofer has warned that if the Chinese tech supplier Huawei is excluded from the country's 5G rollout project, it could be stalled for as long as five or even ten years."); *see also* Ex. FF at 89-97, Mortiz Koch and Dietmar Neuerer, *Interview: CSU-Digitalministerin Bär kritisiert, scheinheilige Huawei-Debatte*, Handelsblatt (Nov. 20, 2019) (Digital State Minister Dorothee Bär stated that Germany does not exclude any particular country or company from the outside and instead focuses on whether certain security standards can be met.); Ex. FF at 151-56, *Angela Merkel Warns EU: "Brexit is a Wake-up Call*," Financial Times (Jan. 16, 2020) (Chancellor Angela Merkel stated that "it is wrong to simply exclude someone per se"). And Italian Minister Stefano Partenelli has advocated for Huawei's participation in Italy's 5G deployment, arguing that "Huawei offers the best solutions at the best prices." Ex. FF at 98-99, *Huawei Should be Allowed 5G Role in Italy: Industry Minister*, Reuters (Dec. 22, 2019).

Elsewhere, South American governments have publicly welcomed Huawei's presence. Brazil's Deputy President, Hamilton Mourão, stated that "Huawei is established in Brazil and will make more investments." Ex. FF at 100-01, *Latin America Resists US Pressure to Exclude Huawei*, Financial Times (June 9, 2019). Marcos Pontes, Brazil's Minister for Science, Technology, Innovation and Communications stated that Brazil will not accept any U.S. pressure to exclude Huawei. Ex. FF at 148-50, Martha Viotti Beck and Simone Preissler Iglesias, *Brazil to Reject U.S. Pressure on Huawei 5G Bid, Minister Says*, Bloomberg News (Jan. 9, 2020). Similarly, Chilean President Sebastián Piñera met with Huawei's Chairman in April and publicly welcomed Huawei to participate in open bidding for 5G development and submarine cable deployment. Ex. FF at 102-04, *Chile to China: Let us be Your Business Hub in Latin America*, Reuters (Apr. 25, 2019). The Indian government, too, recently announced Huawei's participation in trials for 5G

networks. *See* Ex. FF at 105-06, *China's Huawei Gets India Nod to Participate in 5G Trials*, Reuters (Dec. 30, 2019).

Common among the countries that have allowed Huawei products is their rejection of company-specific bans in favor of risk-based approaches and the adoption of cybersecurity best practices to protect their telecommunications networks. These risk-based approaches are consistent with the EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks, which the Commission purported to rely on in designating Huawei. *See* Order ¶ 23 n.160.

Last, the Commission cited communications service providers such as "BT, Orange, and Deutsche Telekom," who, it alleges, are "acting to keep Huawei equipment out of their 5G networks." Order ¶ 53. But this statement is largely false, and otherwise misleading. Deutsche Telekom, which works collaboratively with Huawei, has explained that "[t]he hardware is built to Deutsche Telekom's specifications and is examined by our own security department." Ex. FF at 107-17, Eric Auchard and Sijia Jiang, *China's Huawei Set to Lead Global Charge to 5G Networks*, Reuters (Feb. 23. 2018). Contrary to the Commission's claim that Deutsche Telekom has acted to keep Huawei out of its 5G network due to alleged security concerns, Order ¶ 53, just one week after release of the Order, Deutsche Telekom stated that no such decisions have been made and that it was "not currently entering into any 5G contracts—with any vendor," Ex. FF at 188-121, Douglas Busvine, *Exclusive: Deutsche Telekom Freezes 5G Deals Pending Huawei Ban Decision*, Reuters (Dec. 4, 2019).

Similarly, Huawei continues to work with major carriers abroad, like BT and Orange, both of which the Commission erroneously asserts have cut ties with Huawei in 5G. For example, to support this erroneous assertion, the Commission cited a report by the NATO Cyber Defence Center (the "NATO Cyber Defence Center Paper"), *see* Order ¶ 53 n.166, which in turn cites a news

article from the BBC for the proposition that BT has decided to "abandon Huawei devices," NATO Cooperative Cyber Defence Centre of Excellence, Huawei, 5G, and China as a Security Threat at 17 (2019). However, the *second* paragraph of the cited BBC news article states that "[t]he British firm, however, still plans to use the Chinese company's phone mast antennas and other products deemed not to be at the 'core' of the service." Ex. FF at 122-25, *BT Bars Huawei Kit from Core of 5G Network*, BBC (Dec. 5, 2018). In addition, representatives of BT have said that, although Huawei has not been included in BT's core 5G network, "Huawei remains an important equipment provider outside the core network, and a valued innovation partner," Ex. FF at 126-28, *BT to strip China's Huawei from Core Networks, Limit 5G Access*, Reuters (Dec. 5, 2018), and that, "[o]ver the years that we've worked with Huawei, we've not yet seen anything that gives us cause for concern," Ex. FF at 129-31, Charles Riley and Samuel Burke, *UK telecoms CEO: We've seen no "cause for concern" over Huawei*, CNN (Feb. 8, 2019). Limiting access to the 5G core network is a far cry from keeping "Huawei equipment out of their 5G networks," as the Commission alleged in initially designating Huawei. Order ¶ 53.

With respect to Orange, Huawei was not a supplier to Orange's existing 4G network in France, and Orange CEO Stephane Richard has said simply that Orange is "working with our traditional partners—they are Ericsson and Nokia." Ex. FF at 132-36, Douglas Busvine and Gwénaëlle Barzic, *Deutsche Telekom Reviews Huawei Ties; Orange Says no on 5G*, Reuters (Dec. 14, 2018). Mr. Richard has also publicly questioned the validity of allegations against Huawei, calling the allegations "nonsense." Ex. FF at 137-39, Mathieu Rosemain, *Some Fears about Huawei are 'Complete Nonsense', Orange's Boss Says*, Reuters (Dec. 18, 2019). In the case of the three carriers that the Commission cited, none expressed concerns over the security of Huawei equipment..

4. Huawei's entry into and presence in the U.S. market would *improve*, not threaten, market diversity and security

The Commission claimed that Huawei's "desire to be an end-to-end provider for whole network solutions" equals a "desire to limit diversity in equipment" and that, "when companies 'seek to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries.'" Order ¶ 56 (quotation omitted). As described above, the Commission's evidence on this point was lacking and its reasoning flawed, and the record on this point cannot support designation. *See supra* p. 90. Huawei now submits additional evidence to reinforce this point, including a report from Dr. Debra Aron.

a. Huawei, like the other leading RAN suppliers, offers end-to-end solutions to meet customer needs

While the FCC apparently saw a nefarious motive, the truth is that telecommunications companies, including Huawei, offer end-to-end solutions for the simple reason that customers want them. An end-to-end supplier is one to which a customer can turn to provide all the components of a network (*i.e.*, hardware, software, and services for the core network, RAN, and transport). Aron Report II ¶ 38. An end-to-end solution is valuable to carriers because it offers benefits such as convenience, cost savings, reduced time to market, reduced incompatibility/interoperability costs, and streamlined customer service and problem-solving. *Id.* ¶¶ 38-39 & n.72. Particularly in the "race to 5G," time is of the essence. One study by Nokia Bell Labs Consulting found that "a 5G end-to-end network with an integrated solution from a single prime vendor can reduce total cost of ownership (TCO) by more than 20 percent and decrease time to market by at least 30 percent, compared to multi-vendor solutions." Ex. GG, Press Release, Nokia, Nokia showcases its end-to-end 5G leadership with new Future X Lab in Finland (Sept. 24, 2019).

Responding to the market, other leading telecommunications infrastructure vendors—including Nokia, Ericsson, and Samsung—all publicly state their goal to be an end-to-end provider. Aron Report II ¶¶ 41-43. Samsung boasts about the breadth of its offerings: "Samsung makes all the parts integral to 5G: chips, network equipment, and devices, including smartphones, smart TVs, appliances, and automotive solutions—all with industry-leading security." Ex. HH, Samsung, *Driving a connected world through 5G*. Nokia similarly touts its ability to offer an end-to-end network solution as a competitive advantage. For example, Nokia's 2018 annual report states: "Nokia is a leader in [high-performance end-to-end networks] today and we will use our main competitive advantage—a near-100% end-to-end portfolio that we can deliver on a global scale—to maintain our leadership while managing for profitability." Ex. II, Nokia, Creating the Technology to Connect the World at 8 (May 2019) ("2018 Nokia Annual Report"). Ericsson states that it "offers an end-to-end 5G Platform, across radio, core and transport networks" that "enables operators to roll out and capture new growth opportunities immediately for 5G." Ex. JJ, Ericsson, 5G Deployment Considerations at 15-16 (2018).

Data from the global market further undermines the Commission's claim that Huawei's ability to offer end-to-end network equipment has provided Huawei an advantage over its main competitors. Dr. Aron shows that, in 2018, Huawei's worldwide revenue share among RAN equipment vendors was comparable to those of both Ericsson and Nokia and that RAN equipment revenue shares among the top three vendors vary from region to region outside of North America. Aron Report II ¶ 46-47. Huawei is far from unique in its desire and effort to meet customers' needs for end-to-end network solutions.

b. End-to-end solutions do not require a limitation on equipment diversity

The Commission appears to have equated the offering of an end-to-end solution with a desire to limit the diversity of equipment. For a number of reasons, that inference is unwarranted.

First, a company that offers end-to-end solutions does not necessarily manufacture all components of that solution itself. Aron Report II ¶ 44. Ericsson "deals with around 30,000 suppliers worldwide and their products and services often account for a large part of the deliveries to [its] customers." Ex. KK, Ericsson, About Us. Nokia stated that in 2018, it conducted business with approximately 14,000 suppliers, including "hardware suppliers which cover the materials that go into our products." Ex. LL, Nokia, About Us. Like other telecommunications vendors that offer end-to-end solutions, Huawei designs and manufactures some components for its solution in-house, and relies on an extensive network of over 13,000 suppliers for other components. Nokia 2018 Annual Report at 5; Aron Report II ¶ 44 (describing examples of Huawei's supplier diversity).

Second, end-to-end solutions do not lead to an overall lack of market diversity because customer carriers can and do purchase from multiple providers for their networks, even though they often prefer end-to-end solutions. Aron Report II ¶ 45 (listing examples). As Tom Dowding of Huawei USA explained, "[a]lthough Huawei can provide end-to-end solutions to its customers, it is a common practice in the telecommunications industry to have multi-vendor networks where, for example, equipment procured from one vendor is used in the core network, and another vendor's equipment is used in the RAN." 2/3/2020 Dowding Decl. ¶ 15. In addition, "[p]er the 3GPP standard, within a wireless network, the interfaces between the RAN and core within a wireless network are all standards-based." *Id.* Thus, "there are many cases around the world, including the United States, where the interoperability between Huawei's RAN and a third-party core network

is possible." *Id.* Further, even if each vendor in the United States purchased its entire network from a single vendor, different carriers may choose different vendors, resulting in diversity at the nationwide level. Aron Report II ¶ 46.

Third, as Dr. Aron discusses, the Commission's assertion that Huawei's ability to offer end-to-end services would limit the diversity of network equipment is also inconsistent with the facts of early deployments of 5G globally. *Id.* ¶ 48. Dr. Aron finds that, as of January 2020, Ericsson held 79 commercial 5G agreements or contracts; as of November 2019, Nokia held 50 5G commercial contracts; and as of December 2019, Huawei held 65 commercial 5G contracts. *Id.* She concludes that the continued success of the top three 5G vendors worldwide belies the FCC's concern that, by offering an end-to-end solution, Huawei would reduce diversity of network equipment in the marketplace. *Id*.

c. Huawei's presence would improve, not threaten, competition and diversity

The Commission's arguments regarding market diversity and competition are inconsistent with the facts and market realities.

The Commission claimed that restricting federal funds to Huawei "should unleash competition from more-trusted, higher-quality suppliers in the long run, resulting in significant public interest benefits." Order ¶ 30.[26] That assertion is not supported by basic economic principles, or the facts of the market. Dr. Aron explains that "given how limited Huawei's presence is in the United States currently and has been since it entered the North American market in 2008, the

[26] The Commission appeared to harbor the misapprehension that Huawei's equipment is *lower* in quality than that of its competitors. In both her initial and supplemental reports, however, Dr. Aron explains that Huawei is not a low-quality provider, and that, to the contrary, Huawei is a leader and innovator in the market for RAN equipment. *See* Aron Report I ¶¶ 15, 18, 119-23; Aron Report II ¶¶ 49-54.

purported unleashing of competition due to Huawei's absence would have materialized already." Aron Report II ¶ 17. Instead, the United States has the highest concentration in the market for RAN equipment among all world regions, with just two companies having over three-fourths of sales of RAN equipment in the United States every year since 2010. *Id.* There has been no significant new entrant in the market for RAN equipment between 2008 and 2017. *Id.* ¶ 20; *see also* ¶¶ 17-26 (noting the substantial barriers to entry in the RAN market).

In addition, the Commission said that because "[t]he four largest U.S. mobile carriers do not use and have no plans to use Huawei [] radio access network equipment," its designation of Huawei will not delay U.S. 5G deployment or increase 5G equipment prices, and instead will enable "continued U.S. leadership in 5G." Order ¶ 121. Again, the Commission's reasoning is flawed.

First, the Commission's assertion that its action will not impact the timing of 5G deployment is incorrect. Although the four largest carriers in the United States do not currently utilize Huawei equipment *in the United States*, those carriers' parent companies or subsidiaries that operate networks outside of the United States often use Huawei equipment in their non-U.S. networks. *See* Aron Report II ¶¶ 64-66. These purchasing decisions indicate that, absent U.S. government pressure, these companies presumably would not "forgo an opportunity to use equipment in their networks that is most highly-ranked among competitors and that is successfully deployed by many other major carriers worldwide." *Id.* ¶ 66. In addition, 5G deployment will not exclusively be carried out by the four largest carriers. *See id.* ¶ 67. Indeed, many rural carriers currently use Huawei equipment and the exclusion of Huawei will delay their 5G deployment—impacting tens if not hundreds of thousands of Americans. *See id.* ¶ 68.

Second, the Commission argued that because Huawei has "virtually no business dealings in the U.S." its absence could not impact prices. Order ¶ 121. That assertion is inconsistent with basic economic principles and antitrust policy, which instruct "that even firms with a limited amount of business can exert competitive pressure on prices of other market participants." Aron Report II ¶ 72. That principle applies with special strength in bidding markets, like the market for telecommunications infrastructure. *Id.* ¶ 72. Moreover, the broader policy context of excluding Huawei from the U.S. market, of which the FCC's initial designation is a part, has already had the effect of elevating prices for all carriers relative to what prices would have been if Huawei had been participating in the market at the levels it participates in the rest of the world. *Id.* ¶ 75 (discussing Dr. Aron's initial report, which stated that the upward pricing pressure already caused by Huawei's restriction within the U.S. RAN market, relative to its hypothetical full participation, ranges from 12.6 percent to 16.0 percent). The Commission acknowledged that USF recipients could face higher prices, but claimed, without any support, that such increases would persist only in the "near term." Order ¶ 121. Economic principles tell us otherwise—without any downward pressure on prices from Huawei or other entrants with comparable capabilities, the effects of Huawei's absence from the U.S. market would not abate. Aron Report II ¶ 76.

Third, the Commission's presumption that the United States is a leader in 5G is not supported by the evidence, nor is its statement that Huawei's exclusions would "facilitate" such leadership. *See* Order ¶ 121; *see generally* Aron Report II ¶¶ 79-81 (identifying South Korea as "significantly ahead" and China as rapidly "catch[ing] up" to the United States in its adoption and deployment of 5G). The United States' failure to allocate a mid-band spectrum has translated to slower 5G deployment than other countries and has resulted in "losses to the U.S. economy and employment." Aron Report II ¶ 82. In sum, the exclusion of innovative and large competitors such

as Huawei from the U.S. marketplace not only results in reduced market diversity, but it also increases costs and delays deployment of the country's 5G infrastructure.

Simply put, Huawei would provide the market diversity within the United States that the industry lacks, reducing prices for RAN equipment, facilitating the deployment of 5G, and increasing the diversity of supply (and thus security). In light of this additional evidence, the Commission's reasoning on these points cannot support a final designation.

III. The Bureau cannot enter a final designation without providing Huawei with additional, legally required procedural safeguards

Finally, the Bureau cannot in any event enter a final designation against Huawei without first providing it with additional, legally required procedural safeguards. As Huawei argued before the Commission, the rule should have expressly mandated these protections, and the Commission's initial designation was invalid because it failed to provide them. But even leaving those defects aside, the Bureau is independently required to provide these protections before entering any final designation against Huawei. This final designation proceeding is plainly an adjudication that implicates Huawei's constitutionally protected liberty and property interests and triggers the procedural protections mandated by the Due Process Clause and the APA. And, going forward, the only procedural protection the Bureau appears to contemplate before final designation is an opportunity to file written comments. Order ¶ 98; *see Public Safety & Homeland Security Bureau Announces Comment Date on the Initial Designation of Huawei Technologies Company as a Covered Company in the National Security Supply Chain Proceeding*, Public Notice, PS Docket No. 19-351 (Jan. 3, 2020). But the APA, the Fifth Amendment's Due Process Clause, and the Commission's own regulations guarantee multiple additional, individualized procedural protections before the government can deprive Huawei of its protected liberty and property interests. Thus, even assuming the Commission's initial designation was proper and that there were otherwise a basis for the

Bureau to enter a final designation of Huawei as a "national security threat to the integrity of communications networks or the communications supply chain," it must afford Huawei four additional procedural protections before making that determination.

A. The final designation proceeding threatens Huawei's protected liberty and property interests

The Fifth Amendment's Due Process Clause requires the government to provide "due process" before depriving a person of "liberty" or "property." U.S. Const. amend. V. Three distinct liberty interests would be implicated by any final designation. *First*, the Constitution requires the government to provide due process protections when it injures a person's (including a corporation's) reputation in connection with the denial of a tangible interest. Under the so-called "stigma-plus" test, government action implicates a person's protected liberty interests when it stigmatizes a person's reputation "in connection with the denial of some specific constitutional guarantee or some 'more tangible' interest." *Marrero* v. *City of Hialeah*, 625 F.2d 499, 513 (5th Cir. 1980) (quoting *Paul* v. *Davis*, 424 U.S. 693, 700-02 (1976)); *see also Wisconsin* v. *Constantineau*, 400 U.S. 433, 437 (1971). And it is well-established that the government imposes stigma when it designates an individual or entity a threat to national security. *See, e.g.*, *Nat'l Council of Resistance of Iran* v. *Dep't of State*, 251 F.3d 192, 204 (D.C. Cir. 2010); *Latif* v. *Holder*, 28 F. Supp. 3d 1134, 1151 (D. Or. 2014). Tangible harm includes a change in status, such as loss of status as a government employee, *Dennis* v. *S & S Consol. Rural High Sch. Dist.*, 577 F.2d 338, 343 (5th Cir. 1978); loss of "business goodwill" where such goodwill is protected by law, *Marrero*, 625 F.2d at 514-15; and loss of opportunity to operate one's business, *Texas* v. *Thompson*, 70 F.3d 390, 393 (5th Cir. 1995). Similarly, an entity may demonstrate a "constitutionally cognizable interest in avoiding the loss of government contracting opportunities based on stigmatizing charges," even where the

stigmatizing government action does not amount to actual debarment from "virtually all government work for a fixed period of time." *Reeves Aleutian Airways, Inc.* v. *United States*, 982 F.2d 594, 598 (D.C. Cir. 1993) (quotation marks omitted).

Second, the Due Process Clause protects a person's "liberty interest in pursuing a chosen occupation." *Stidham* v. *Tex. Comm'n on Private Sec.*, 418 F.3d 486, 491 (5th Cir. 2005); *see also, e.g.*, *Greene* v. *McElroy*, 360 U.S. 474, 492 (1959). Thus, the Clause requires meaningful procedural protections when the government takes action that "broadly precludes individuals or corporations from a chosen trade or business." *Trifax Corp.* v. *District of Columbia*, 314 F.3d 641, 644 (D.C. Cir. 2003).

Third, the Due Process Clause protects a person's liberty interest against debarment from government programs without due process. Debarment from service as a government contractor is a deprivation of liberty, regardless of whether the debarment is formal or instead the result of reputational harm. *Trifax*, 314 F.3d at 643-44; *see, e.g.*, *Bank of Jackson Cty.* v. *Cherry*, 980 F.2d 1354, 1359 (11th Cir. 1992). Government action in the debarment context implicates protected liberty interests when the government "excludes [a person] from work on some category of future [government] contracts or from other government employment opportunities," thereby "chang[ing]" the person's "formal legal status." *Kartseva* v. *Dep't of State*, 37 F.3d 1524, 1528 (D.C. Cir. 1994). In addition, the government deprives a person of liberty when it takes a debarment action that "has the *broad* effect of largely precluding [the person] from pursuing [a] chosen career." *Id.*; *see Trifax*, 314 F.3d at 643-44. Similar principles apply in "de facto licensing" cases, where private industry will not employ a person without government approval. *See Phillips* v. *Vandygriff*, 711 F.2d 1217, 1222 (5th Cir. 1983). In those cases, "[t]he freedom to pursue any of the 'common occupations' has long been held to be a liberty interest." *Id.* at 1223.

Any final designation entered against Huawei would deprive it of all three of these protected liberty interests. *First*, by designating Huawei a threat to national security and effectively prohibiting it from competing for contracts to be fulfilled using USF funds, any final designation would stigmatize Huawei, brand it with a badge of infamy, and tangibly alter its legal and practical ability to contract with USF recipients. The Commission itself concedes that "designation by the Commission as a threat to national security is likely to impose some amount of stigma." Order ¶ 102 & n.277. And a final designation would alter Huawei's tangible interests by both legally and practically prohibiting it from competing for contracts to be fulfilled by USF funds.

The Commission claims that designation would impose "no explicit restriction on designated entities at all." *Id*. ¶ 103. But the plain and intended effect of a final designation would be to preclude Huawei from entering into contracts that involve use of USF funds. The stigma imposed by a designation would also tangibly harm Huawei's business opportunities and goodwill. Indeed, former Huawei customers have canceled orders and contracts and ceased negotiations with Huawei. 7/2/2018 Huawei Reply Comments at 24-25; 6/1/2018 Dowding Decl. ¶ 33. Furthermore, even though a final designation would, by its terms, only affect use of USF funds, it would effectively bar use of Huawei products and services on most or all projects undertaken by USF recipients. As the Commission itself concedes, it is "unlikely that many USF recipients will be able to show the detailed records necessary to demonstrate that no USF funds were used on equipment or services from a covered company on any part of the project." Order ¶ 72. In addition, there is no serious doubt that the stigma of being designated a national security threat to communications networks and the communications supply chain will discourage *all* potential customers—whether USF recipients or not—from purchasing and using Huawei equipment.

Second, final designation would deprive Huawei of its liberty to operate its business and pursue its chosen occupation. Final designation is designed to stop designated entities from receiving USF funds based on the determination that those entities are threats to the communications network and supply chain. The effect of such a designation is clear: Huawei will lose business. Indeed, in response to the NPRM, a number of Huawei's customers canceled purchase orders, stopped paying for equipment and services already provided, and suspended projects and contract negotiations. 7/2/2018 Huawei Reply Comments at 24-25.

Third, final designation would debar Huawei from participating in a government program as a supplier of equipment to USF fund recipients—again implicating a protected liberty interest. The Commission contends that designation does not "completely prevent entities from transacting with carriers who receive USF funding." Order ¶ 101. But debarment does not require complete exclusion from all government-related opportunities. A final designation would prevent Huawei from contracting for a "definite range" of government-funded opportunities, *Kartseva*, 37 F.3d at 1527, and that deprivation is sufficient to implicate liberty interests and trigger the protections of the Due Process Clause. The debarment principle also applies regardless of whether a company directly contracts with the government or serves as a subcontractor. Indeed, the Fifth Circuit has held that the government infringes the liberty interest in practicing one's occupation when it withholds a license—or even simply approval—that industry custom regards as important to private hiring decisions. *Phillips*, 711 F.2d at 1222.

Liberty interests aside, the Due Process Clause requires the government to provide "due process" before depriving a person of "property." U.S. Const. amend. V; *see Board of Regents* v. *Roth*, 408 U.S. 564, 577 (1972). Rights under existing contracts are constitutionally protected property interests. *See, e.g.*, *Mid-Am. Waste Sys., Inc.* v. *City of Gary*, 49 F.3d 286, 290 (7th Cir.

1995); *cf. Sierra Club* v. *Espy*, 18 F.3d 1202, 1207 (5th Cir. 1994). Huawei thus has protected property interests in its existing contracts with USF recipients and suppliers to USF recipients. *See, e.g.*, Groft Decl. ¶ 3 (referencing James Valley Telecommunications' contracts with Huawei); Comments of Sagebrush Cellular, Inc., WC Docket No. 18-89, at 2 (filed June 1, 2018) (discussing Sagebrush's contracts with Huawei). Consequently, the Commission cannot take action to interfere with, let alone effectively abrogate through the designation process, those existing contracts without providing affected companies the process that the Fifth Amendment requires. *Cf. Roth*, 408 U.S. at 569-70. Yet a final designation under the USF rule would destroy those protected contracts. *See* Order ¶¶ 72, 87.

B. Additional procedures are required before a final designation can be entered

Because a final designation would deprive Huawei of its constitutionally protected liberty and property interests, the Due Process Clause requires the Bureau to provide it with certain procedural protections prior to any such designation. To begin with, Huawei is entitled to formal adjudication procedures under the APA. *See* 5 U.S.C. §§ 554, 556-57. Those procedures are triggered when, like here, the Due Process Clause requires a hearing. *Wong Yang Sung* v. *McGrath*, 339 U.S. 33, 49 (1950); *see also United States* v. *Mead Corp.*, 533 U.S. 218, 243 (2001) (Scalia, J., dissenting); *Collord* v. *U.S. Dep't of Interior*, 154 F.3d 933, 936 (9th Cir. 1998); *see also* 5 U.S.C. §§ 554, 556-57 (listing required procedural protections, including notice of the matters of fact and law asserted, an opportunity to submit facts and arguments in response, an opportunity to conduct necessary cross-examination, an impartial decisionmaker, and a proceeding free from ex parte communications). The Bureau must thus conduct a formal adjudication proceeding before it can enter any final designation against Huawei.

Apart from the APA, the Due Process Clause independently requires that Huawei receive at least four important procedural protections in the course of any adjudication leading to a final

designation. *See Wong Yang Sung*, 339 U.S. at 49; *Mathews* v. *Eldridge*, 424 U.S. 319, 335 (1976). To determine which procedural protections are due, courts balance "the private interest that will be affected by the official action," "the risk of an erroneous deprivation of such interest through the procedures used," and "the Government's interest, including the … burdens that the additional or substitute procedural requirement would entail." *Mathews*, 424 U.S. at 335. Here, under that balancing test, Huawei is entitled to (1) notice of the evidence against it and the Bureau's reasons for believing that evidence warrants final designation; (2) an opportunity to respond to the evidence, including the right to cross-examine any witnesses against it; (3) an impartial decisionmaker unaffected by bias, prejudice, or prejudgment; and (4) proceedings free from ex parte contacts.

More specifically, the "private interest that will be affected" by a final designation, 424 U.S. at 335, is extremely significant here: as discussed, a final designation entered against Huawei would directly deprive it of its ability to sell equipment and services that will be paid for with USF funds, and indirectly (but predictably) deprive it of its ability to sell equipment and services to USF recipients even when they are not using USF funds, and will impose a stigma on Huawei that will affect its ability to do business with other potential customers. There is a serious risk that Huawei will be "erroneous[ly] depriv[ed]" of this interest absent the four additional procedural protections, *id.*, because, as discussed below, each of them is critical to ensuring that the Bureau has before it a developed record that gives Huawei a full opportunity to respond to the accusations and evidence against it, and that the Bureau has implemented safeguards to ensure that the decisionmaking process is untainted and free from unfair bias. And the Government also has an affirmative interest in providing these protections, in order to ensure that it imposes restrictions only pursuant to a fair and complete process. Further, any administrative burden that would arise from providing these protections would be minimal, and would be easily outweighed by the benefit to

Huawei and the Bureau itself. Here, Huawei is entitled to at least four protections under this balancing test.

First, Huawei is entitled to disclosure of the evidence to be used against it and an opportunity to show that the evidence is untrue. *See, e.g.*, *Greene*, 360 U.S. at 477-79, 496, 507; *Ralls Corp.* v. *CFIUS*, 758 F.3d 296, 318 (D.C. Cir. 2014). Without notice of the evidence on which the Bureau intends to rely, or an understanding of how that evidence satisfies the criteria announced by the Commission, Huawei cannot compile a full and responsive record for the Bureau or provide an appropriate rebuttal to its conclusions.

To be clear, the Commission's Order and the initial designation within it do not provide Huawei with the required notice. As Huawei has explained to the Commission, the Commission's rule provides no criteria to guide its application, and Huawei had (and has) no notice of the standard that the Commission applied against it in rendering its initial designation (to the extent that there was any discernible standard at all)—much less the standard that the Bureau might apply going forward. *See supra* pp. 2-4, 8-11, 25-27. Further, the Commission has introduced no actual evidence against Huawei—at least none that is probative of anything apparently material under the standardless rule (so far as Huawei can tell, given the rule's lack of any meaningful or measurable criteria). Before this final designation proceeding may go any farther, the Bureau must inform Huawei of the standard to be applied, how any criteria are to be measured, and what evidence it believes satisfy those criteria. Huawei recognizes that, because the Commission has provided no guidance as to the standard to be applied under the rule, it has left the Bureau in a difficult position with respect to this requirement. Nonetheless, it would violate the due process guarantee for the Bureau to enter a final designation against Huawei without giving it notice of the standards being applied to it or the evidence that purportedly satisfies those standards. In addition, to ensure that

Huawei has adequate notice of the evidence against it, the Bureau may not rely "critically" on classified information to support a final designation. *People's Mojahedin Org.*, 613 F.3d at 231. At the very least, the Bureau must disclose any classified information on which it intends to rely "ex parte and in camera" to a neutral adjudicator to determine what portions of that material may be disclosed to Huawei in a redacted form. *Holy Land Found. for Relief & Devel.*, 333 F.3d at 164.

Second, the Bureau must give Huawei a fair opportunity to respond to the evidence on which it intends to rely, including the right to cross-examine any witnesses against it. *See Greene*, 360 U.S. at 496-97; *Ching* v. *Mayorkas*, 725 F.3d 1149, 1158 (9th Cir. 2013) (citing *Goldberg* v. *Kelly*, 397 U.S. 254, 269 (1970)); *Bus. Commc'ns, Inc.* v. *U.S. Dep't of Educ.*, 739 F.3d 374, 380 (8th Cir. 2013); *Cooper* v. *Salazar*, 196 F.3d 809, 815 (7th Cir. 1999); 5 U.S.C. § 556(d). Thus, to the extent the Bureau intends to consider the hearsay-based conclusions in the HPSCI Report in its final designation proceeding against Huawei—and it should not, for the reasons discussed above, *see supra* pp. 59-72—the Bureau must provide Huawei with an opportunity to disprove the report's conclusions by, among other things, cross-examining the sources on which the report relies. And to the extent the Bureau considers any other witness testimony, the Bureau must afford Huawei the opportunity to cross-examine those witnesses and rebut their claims as well. The existence of a dispute over several issues of material fact demonstrates the necessity of cross-examination that would aid the Bureau to come to a decision based on fact rather than speculation and innuendo. For example:

(1) The Commission claimed—but Huawei disputes—that "Huawei's founder, Ren Zhengfei, is himself believed to be a former director of the People's Liberation Army Information Engineering Academy, an organization associated with China's signals intelligence." Order ¶ 50 (citing HPSCI Report at 13-14, which in turn relied on "[m]any industry analysts"); *see supra* pp.

83-84, 131-34. Before any final designation, Huawei must have the opportunity to cross-examine those "industry analysts" to probe what possible personal knowledge or other purported basis they could have had for such a claim.

(2) The Commission relied on a report issued by Finite State to assert that Huawei had a "high number" of security vulnerabilities. Order ¶ 54. Huawei disputes the propriety of such reliance. *See supra* pp. 78-80. Before any final designation, Huawei must have the opportunity to cross-examine individuals at Finite State who purportedly tested Huawei's products in order to probe their alleged qualifications, how they conducted their testing, what specific equipment was tested, and how they reached their conclusions, among other questions. "Because experts are often less than helpful and sometimes misleading, effective cross-examination by an opposing party is an essential tool for exposing any weaknesses in the expert's opinions." *Trigon Ins. Co.* v. *United States*, 204 F.R.D. 277, 289 (E.D. Va. 2001); *Daubert* v. *Merrell Dow Pharm., Inc.*, 509 U.S. 579, 596 (1993).

(3) The Commission claimed, citing a report written by a Priscilla Moriuchi, that Huawei "generates a nearly unimaginable amount of data for one company to possess" and that Huawei has "access to this vast amount of data." Order ¶ 56. Huawei disputes this hyperbolic assertion and its relevance. (Huawei cannot access customer data without consent. *See supra* pp. 46-49, 146-49.) Before any final designation, Huawei must have the opportunity to cross-examine Ms. Moriuchi to probe what possible qualifications she could have and what personal knowledge or other purported basis she could have had for such a claim.

(4) The Commission claimed that "[t]he House Permanent Select Committee on Intelligence … received internal Huawei documentation from Huawei employees 'showing that Huawei provides special network services to an entity the employee believes to be an elite cyber-warfare

unit within the PLA.'" Order ¶ 50. Huawei disputes that it provided any such services. *See supra* pp. 66-68, 130-31. Before any final designation, Huawei must have the opportunity to cross-examine those "Huawei employees" to probe what possible personal knowledge or other basis they could have had for that claim.

(5) The Commission claimed that "analysts have found that while 'Huawei claims the Chinese state has no influence over its activities, … the company is treated as a state-owned enterprise and has benefited from state procurement funds, subsidized financing from state-owned policy banks and state funding for research.'" Order ¶ 51. Huawei disputes the assertion. *See supra* pp. 42-46, 83-87, 127-31, 139-42. Before any final designation, Huawei must have the opportunity to cross-examine those "analysts" to probe what possible personal knowledge or other purported basis they could have had for that claim.

(6) The Commission claimed that "the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions." Order ¶ 50 (citing the HPSCI Report at 23, which in turn relied on "experts in Chinese political economy"). Huawei disputes that the internal Communist Party Committee plays any such role. As explained above, the committee plays no role in daily operations of the company or in deciding major issues. *See supra* pp. 43-44, 84, 134-39. Before any final designation, Huawei must have the opportunity to cross-examine the purported "experts in Chinese political economy" to probe what possible qualifications or basis for their conclusions they could have had, including any basis of knowledge specific to the internal Party Committee at Huawei.

(7) The Commission expressly relied on the decisions of other countries to exclude Huawei, citing decisions made by the governments of New Zealand, Japan, and Australia. Order ¶ 53. Huawei disputes the propriety of such reliance. *See supra* pp. 51-54, 149-55. Before any final

designation, Huawei must have the opportunity to cross-examine the representatives from those countries that have excluded Huawei to probe the reasons for the decisions and to determine whether those countries conducted an objective, independent security risk assessment and what the specifics of such an assessment were. As Huawei has explained, the Commission has not shown that those decisions were not simply policy choices responding to U.S. government pressure, rather than objective threat assessments. *See supra* pp. 53-54, 150-52.

Absent cross-examination on these and other disputed issues, the Bureau cannot reach a final designation that comports with due process.

Third, the Bureau must ensure that the final designation proceedings are conducted by an impartial decisionmaker who will render a decision unaffected by bias, prejudice, or prejudgment. *See Wong Yang Sung*, 339 U.S. at 50; *Fogo de Chao*, 769 F.3d at 1148; *Metro. Council of NAACP Branches* v. *FCC*, 46 F.3d 1154, 1164-65 (D.C. Cir. 1995); *ATX, Inc.*, 41 F.3d at 1527; *DCP Farms*, 957 F.2d at 1188; *Pillsbury Co.*, 354 F.2d at 954-56; *Koniag*, 580 F.2d at 610; *Latecoere Int'l, Inc.*, 19 F.3d at 1356; Ex. 1-H, Hammond Decl. at 9-14. As an initial matter, if any members of the Bureau have made public statements demonstrating bias or prejudice toward Huawei or prejudgment of Huawei's status under the USF rule, those decisionmakers must be disqualified from participation in the final designation proceeding. *See Cinderella*, 425 F.2d at 590. Similarly, if any members of the Bureau make statements creating the appearance of impartiality *during* the final designation proceeding, the Bureau must restart the proceeding anew without the participation of the biased decisionmakers. *Id.* Otherwise, the entire final designation proceeding will be tainted by prejudgment bias because there will be "no way of knowing" precisely how an individual decisionmaker's "participation affected the [Bureau's] deliberations." *Antoniu*, 877 F.2d at 726. More fundamentally, if anyone in the Bureau working on the designation has "made up his

mind … and is impervious to contrary evidence," *Fogo de Chao*, 769 F.3d at 1148—whether because the Commission has already indicated that it expects the Bureau to rubber stamp its initial designation, or otherwise—then he must be disqualified as well.

Fourth, the Bureau must order that the final designation proceeding remain free of ex parte contacts. Indeed, the Commission's own regulations require an order prohibiting ex parte contacts, because the designation proceedings are properly considered "restricted." 47 C.F.R. § 1.1208. The regulations governing ex parte contacts specify that a proceeding may be either "restricted," "permit-but-disclose," or "exempt." *Id.* § 1.1200. Ex parte contacts "are prohibited" in restricted proceedings, which are defined as a residual category comprising "all proceedings not listed as exempt … or permit-but-disclose." *Id.* § 1.1208. The regulations list six categories of exempt proceedings, such as a "notice of inquiry" and a "petition for rulemaking." *Id.* § 1.1204(b). The regulations also list thirteen categories of permit-but-disclose proceedings, such as an "informal rulemaking" and "a proceeding involving a rule change, policy statement or interpretive rule." *Id.* § 1.1206(a). But the designation proceedings fit within none of the enumerated categories. They are therefore "restricted" proceedings, in which ex parte contacts are forbidden. This protection is important because, as was noted above, there have been significant ex parte contacts with the Commission that have already cast doubt on the neutrality and validity of these proceedings. *See supra* pp. 23-24.

If there were any doubt, constitutional concerns and good adjudicatory practices militate strongly for categorizing the designation proceedings as restricted. Courts have held that the due process guarantee also operates as a prohibition on ex parte contacts. *See U.S. Lines, Inc.* v. *Fed. Maritime Comm'n*, 584 F.2d 519, 536-40 (D.C. Cir. 1978); *Sangamon Valley Television Corp.* v. *United States*, 269 F.2d 221, 224 (D.C. Cir. 1959)*; see also United States* v. *Fla. E. Coast Ry.*, 410 U.S. 224, 245 (1973); 5 U.S.C. § 557(d)(1)(B); *Sierra Club* v. *Costle*, 657 F.2d 298, 400 (D.C.

Cir. 1981). Here, if interested parties were permitted to lobby the Bureau with new and undisclosed arguments—which Huawei cannot possibly anticipate or otherwise rebut—it would undermine the entire purpose of the notice requirement and violate norms of "basic fairness." *Sangamon Valley Television Corp.*, 269 F.2d at 224; *see also, e.g.*, *Fla. E. Coast Ry.*, 410 U.S. at 245; *U.S. Lines*, 584 F.2d at 536-40; *Sierra Club*, 657 F.2d at 400. The protection against secret ex parte contacts is particularly important in light of the overwhelming political pressures exerted on the Commission to designate Huawei in the first place. *See supra* pp. 8-11, 115-20 (detailing the record of congressional interference with the Commission's rulemaking and initial designation of Huawei). To ensure that its decision is not influenced by covert communications and undisclosed political pressures, the Bureau must prohibit ex parte communications during its final designation proceeding against Huawei.

To be sure, the Commission maintains discretion to "modify the applicable ex parte rules" for a particular proceeding by "order, letter, or public notice." 47 C.F.R. § 1.1200(a). But that exception is inapplicable here for two reasons. First, the due process principles just discussed independently require a process free from ex parte contacts. Second, as to the final designation proceeding, the Commission has not modified the applicable rules by designating it as a permit-but-disclose proceeding. *Id.* § 1.1200. There is nothing about ex parte rules for the final-designation proceeding in the Order issued November 26, 2019. The Order designated as "permit-but-disclose" the "proceeding this Further Notice initiates," but the only proceeding the "Further Notice" initiated was the rulemaking regarding equipment removal and reimbursement. Order ¶ 177; *see also* Order ¶ 122 & Part IV ("Further Notice"). The Order as published in the Federal Register states that "[t]his proceeding shall be treated as a 'permit-but-disclose' proceeding," apparently referring to the final designation proceeding. 85 Fed. Reg. 249 ¶ 137. But the legal effect of an FCC order

must be based on the actual text released by the Commission, not by a summary published in the *Federal Register*.

CONCLUSION

For the reasons set forth above, the Bureau should decline to enter a final designation against Huawei.

Respectfully submitted,

Glen D. Nager
Michael A. Carvin
Shay Dvoretzky

JONES DAY
51 Louisiana Ave., NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
macarvin@jonesday.com
sdvoretzky@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

Counsel to Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc.

February 3, 2020

LIST OF EXHIBITS

Exhibit A	Declaration of Timothy Danks
Exhibit B	Declaration of Thomas Dowding
Exhibit C	Declaration of Alan Fanzhiyong
Exhibit D	Declaration of William Zheng
Exhibit E	Declaration of Leon Wang
Exhibit F	Declaration of Wei Jiang
Exhibit G	Expert Report of Randall Peerenboom
Exhibit H	Expert Report of Wei Jiang, Ph.D.
Exhibit I	Supplemental Expert Report of Dr. Debra J. Aron
Exhibit J	7/3/2012 Huawei First Responses to HPSCI
Exhibit K	9/22/2012 Huawei Second Responses to HPSCI
Exhibit L	Affidavit of David He, *Huawei Technologies USA, Inc., et al. v. United States*, No. 4:19-cv-00159 (E.D. Tex.)
Exhibit M	Ex. 71 to Huawei Motion for Summary Judgment, *Huawei Technologies USA, Inc., et al. v. United States*, No. 4:19-cv-00159 (E.D. Tex.)
Exhibit N	Premier Li Keqiang Meets the Press: Full Transcript of Questions and Answers, State Council of the People's Republic of China (Mar. 15, 2019)
Exhibit O	Transcript, *Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on December 17, 2019*, Ministry of Foreign Affairs of the People's Republic of China (Dec. 17, 2019)
Exhibit P	*Banning Huawei would leave Britain trailing behind on technology,* Telegraph (Jan. 4, 2020)
Exhibit Q	*Yang Jiechi: Hope the United States (US) Side Will Work with the Chinese Side to Well Implement the Consensus of the Two Heads of State and Promote Bilateral Relations Based on Coordination, Cooperation and Stability*, Embassy of the People's Republic of China in the United States of America (Feb. 17, 2019)

Exhibit R	*Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on February 18, 2019*, Ministry of Foreign Affairs of the People's Republic of China (Feb. 18, 2019)
Exhibit S	*Huawei founder Ren Zhengfei denies firm poses spying risk*, BBC News (Jan. 15, 2019)
Exhibit T	John Eggerton, *FCC's Pai to Senate: Huawei is National Security Threat*, Broadcasting+Cable (May 8, 2019)
Exhibit U	Press Release, Cotton and Rubio Introduce Legislation to Prohibit U.S. Government Use of Chinese Telecommunications Companies (Feb. 7, 2018)
Exhibit V	Press Release, Ruppersberger, Rogers Warn U.S. Companies Doing Business With Huawei, ZTE (Oct. 11, 2012)
Exhibit W	Brendan Carr (@BrendanCarrFCC), Twitter (Oct. 28, 2019, 12:34 PM)
Exhibit X	Geoffrey Starks, *The Huawei threat is already here*, TheHill (May 26, 2019)
Exhibit Y	Nilay Patel & Makena Kelly, *FCC Commissioner Geoffrey Starks talks Huawei and net neutrality on The Vergecast*, TheVerge.com (May 21, 2019)
Exhibit Z	Marguerite Reardon, *FCC commissioner wants Huawei gear out of US networks*, CNET (Jun. 22, 2019)
Exhibit AA	Margot James, *The Evidence Available Does Not support a Total Ban on Huawei*, Conservative Home (Jan. 24, 2020)
Exhibit BB	Charles Arthur, *China's Huawei and ZTE Pose National Security Threat, says US Committee,* Guardian (Oct. 8, 2012)
Exhibit CC	Jim Wolf, *U.S. Lawmakers Seek to Block China Huawei, ZTE U.S. Inroads*, Reuters (Oct. 7, 2012)
Exhibit DD	Simon Montlake, *U.S. Congress Flags China's Huawei, ZTE as Security Threats*, Forbes (Oct. 8, 2012)
Exhibit EE	*Huawei and ZTE: Put on Hold*, The Economist (Oct. 13, 2012)
Exhibit FF	Collection of Reports Detailing International Use of Huawei Equipment and Services

Exhibit GG	Press Release, Nokia, Nokia showcases its end-to-end 5G leadership with new Future X Lab in Finland (Sept. 24, 2019)
Exhibit HH	Samsung, *Driving a connected world through 5G*
Exhibit II	Nokia, Creating the Technology to Connect the World (May 2019)
Exhibit JJ	Ericsson, 5G Deployment Considerations (2018)
Exhibit KK	Ericsson, *About Us*
Exhibit LL	Nokia, *About Us*
Exhibit MM	Huawei, *Independent Auditor*
Exhibit NN	Zen Soo, *Huawei Is in Better Shape to Withstand US Pressure, Thanks to Industry's Largest Research Budget*, South China Morning Post (Apr. 26, 2018)
Exhibit OO	Gei Tai, Civil Engineering Corps, *Ren Zhengfei*, Oct. 18, 1978
Exhibit PP	Wenhui Bao, China's first high-precision measuring quasi-equipment, Oct. 14, 1977
Exhibit QQ	Huawei Investment & Holding Co., Ltd. 2018 Annual Report
Exhibit RR	Huawei, *Huawei Completes BSIMM Assessment of its Industry-Leading Software Security Capabilities* (June 8, 2018)
Exhibit SS	Plaintiff's Motion for Summary Judgment, *Huawei Techs. USA, Inc. v. United States*, No. 4:19-cv-00159-ALM (E.D. Tex. Filed Mar. 6, 2019)
Exhibit TT	Finnvera, *Buyer financing arranged through cooperation between export credit agencies*
Exhibit UU	Affidavit of Li Xu, *Huawei Technologies USA, Inc., et al.* v. *United States*, No. 4:19-cv-00159 (E.D. Tex.)
Exhibit VV	2/3/2020 Certification and Testing of Huawei Products

Previous Submissions in WC Docket No. 18-89

Exhibit 1	6/1/2018 Huawei Comments to the Proposed Rulemaking
Exhibit 1-A	Declaration of John Suffolk
Exhibit 1-B	Declaration of Donald A. Purdy, Jr.
Exhibit 1-C	Declaration of Thomas Dowding
Exhibit 1-D	Declaration of Ariel Ye
Exhibit 1-E	Declaration of Jihong Chen and Jianwei Fang
Exhibit 1-F	Declaration of Allan L. Shampine
Exhibit 1-G	Declaration of Bryant Tow
Exhibit 1-H	Declaration of Emily Hammond
Exhibit 1-I	Huawei Cyber Security White Paper June 2016
Exhibit 1-J	Huawei Cyber Security White Paper December 2014
Exhibit 1-K	Huawei Cyber Security White Paper October 2013
Exhibit 1-L	Huawei Cyber Security White Paper September 2012
Exhibit 1-M	"Nokia Signing a Joint Venture Agreement with China Huaxin to Establish Nokia Shanghai Bell"
Exhibit 1-N	"Nokia 2016 Corporate Social Responsibility Report of Shanghai Nokia Bell"
Exhibit 1-O	Certification and Testing of Huawei Products
Exhibit 2	7/2/2018 Huawei Reply Comments to the Proposed Rulemaking
Exhibit 2-A	Reply Declaration of Donald Purdy, Jr.
Exhibit 2-B	Letter to Representatives J. Boehner, H. Reid, N. Pelosi, and M. McConnell (April 4, 2013)
Exhibit 2-C	Reply Declaration of Thomas Dowding
Exhibit 2-D	Reply Declaration of Allan L. Shampine

Exhibit 3	8/6/2018 Huawei Ex Parte (responding to Comments from the Telecommunications Industry Association)
Exhibit 3-A	Expert Report of Jacques DeLisle
Exhibit 3-B	Supplemental Expert Report of Jihong Chen and Jianwei Fang
Exhibit 3-C	Huawei Letter to TIA, June 15, 2018
Exhibit 3-D	2017 Market Share and Concentrated Data: Selected Excerpts
Exhibit 3-E	Nokia Annual Report on Form 20-F 2017
Exhibit 3-F	List of State-Owned Enterprises
Exhibit 3-G	"People-oriented Science and Technology Nokia-Bell Takes the Lead in 5G Technology."
Exhibit 3-H	"Enterprise Party Organization Oriented Toward Directing, Team Building, and Atmosphere Fostering"
Exhibit 3-I	Nokia Shanghai Bell 2017 Corporate Social Responsibility Report
Exhibit 3-J	WTO Report WT/GC/W/745
Exhibit 3-K	"State-owned Enterprise Staffing Adjustment"
Exhibit 3-L	"Zhang Qi from Nokia-Bell China Will Certainly Lead the 5G Era"
Exhibit 3-M	"Why Nokia Chooses Hangzhou to Build Its Largest R&D Center in China"
Exhibit 4	8/23/2018 Huawei Ex Parte (describing the Huawei Cyber Security Evaluation Centre)
Exhibit 5	8/27/2018 Huawei Ex Parte (incorporating Huawei's Comments before the FTC)
Exhibit 5-A	Attachment, Huawei's Comments to the Federal Trade Commission, 8/20/2018
Exhibit 6	10/1/2018 Huawei Ex Parte (disclosing a meeting between the FCC, Huawei, Morgan Lewis, and Jones Day)
Exhibit 6-A	September 28, 2018 Meeting Attendees
Exhibit 6-B	June 2, 2018 Selected Quotes in the Record

Exhibit 7	11/16/2018 Huawei Comments (addressing Section 889 of the National Defense Authorization Act ("NDAA"))
Exhibit 8	12/7/2018 Huawei Reply Comments (addressing Section 889 of the NDAA)
Exhibit 9	1/28/2019 Huawei Ex Parte (responding to comments from the TIA)
Exhibit 10	2/15/2019 Huawei Ex Parte (addressing the Supply Chain Security Act)
Exhibit 11	3/12/2019 Huawei Ex Parte Submission (addressing federal telecommunications policy and enclosing a copy of Huawei's E.D. Tex. Complaint)
Exhibit 11-A	Complaint, *Huawei Technologies USA, Inc. et al. v. United States*, No. 4:19-cv-00159-ALM (E.D. Tex.)
Exhibit 12	5/10/2019 Huawei Ex Parte (providing expert report on China's Cyber Security Law)
Exhibit 12-A	Expert Report of Dr. Hanhua Zhou
Exhibit 13	6/12/2019 Huawei Ex Parte (addressing the targeting of specific vendors)
Exhibit 14	9/18/2019 Huawei Ex Parte (providing exhibits related to other telecommunications companies with connections to China)
Exhibit 14-A	"Company Profile" of Panda Electronics Group Co. Ltd.
Exhibit 14-B	Ericsson's "About Us: China" Webpage
Exhibit 14-C	"Ericsson Preserves Competitiveness on 5G Development in China"
Exhibit 14-D	"Ericsson: Things are Getting Better"
Exhibit 14-E	Excerpts from LM Ericsson Telephone Co.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018
Exhibit 14-F	Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018
Exhibit 14-G	Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year 2017
Exhibit 14-H	Excerpts from China Mobile Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Exhibit 14-I	"FCC Denies China Mobile's Bid to Provide International Telecom Services in the U.S."
Exhibit 14-J	"Company Overview" of China Telecom (Americas)
Exhibit 14-K	Excerpts from China Telecom Corp. Ltd.'s Form 20-F Annual Report for Fiscal Year 2018
Exhibit 14-L	Excerpts from China Unicom (Hong Kong) Ltd.'s Form 20-F Annual Report for Fiscal Year 2018
Exhibit 14-M	"Nokia Corp., Nokia and China Huaxin Sign Definitive Agreements for Creation of New Nokia Shanghai Bell Joint Venture"
Exhibit 14-N	"Finnish Visit to Nokia Shanghai Bell"
Exhibit 14-O	"NSA Concerns Give Chinese Server Maker a Boost"
Exhibit 14-P	PC Magazine's Online Product-Overview Page for Cisco Systems, Inc.'s Catalyst 3650-48P Layer 3 Switch
Exhibit 14-Q	Excerpts from Cisco Systems, Inc.'s Form 10-K Annual Report for Fiscal Year Ended July 30, 2016
Exhibit 14-R	Excerpts from Hewlett Packard Enterprise Co.'s Form 10-K Annual Report for Fiscal Year Ended Oct. 31, 2018
Exhibit 14-S	"Magic Quadrant for LTE Network Infrastructure"
Exhibit 14-T	Excerpts from Lenovo Group Ltd.'s 2017/18 Annual Report
Exhibit 14-U	"USA Smartphone Market Share: By Quarter"
Exhibit 14-V	"DoD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices"
Exhibit 14-W	Backgrounder, Alcatel-Lucent Enterprise
Exhibit 14-X	Alpha Networks, Inc.'s "Design Manufacturing, Service (DMS)" Webpage
Exhibit 14-Y	Alpha Networks, Inc.'s "About Alpha" Webpage
Exhibit 14-Z	Excerpts from Arista Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year 2018
Exhibit 14-AA	Excerpts from Extreme Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended June 30, 2018

Exhibit 14-BB	Excerpts from Juniper Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended Dec. 31, 2018
Exhibit 14-CC	"OnePlus Breaks Into Top 5 Premium Phone Makers in US Market"
Exhibit 14-DD	"Who is BBK, The World's Third Largest Phone Manufacturer?"
Exhibit 14-EE	"Meet the 'Godfather' of China's Smartphone Industry"
Exhibit 14-FF	"China's Tsinghua Unigroup to Build $30 Billion Memory-Chip Factory in Nanjing"
Exhibit 14-GG	Tsinghua Holdings Co. Ltd.'s "Products and Technological Services" Webpage
Exhibit 14-HH	"Shenzhen Government Takes Control of China's Leading Chip Maker Tsinghua Unigroup"
Exhibit 14-II	"Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology" by Interos Solutions, Inc.
Exhibit 15	10/11/2019 Huawei Ex Parte (providing an expert report analyzing the economic impact of excluding Huawei from the U.S. market)
Exhibit 15-A	Expert Report of Dr. Debra J. Aron
Exhibit 16	10/31/2019 Huawei Ex Parte (rebutting the Finite State Report)
Exhibit 16-A	"Finite State Report Fails to Tell the Whole Story"
Exhibit 16-B	Huawei PSIRT: Technical Analysis Report Regarding Finite State Supply Chain Assessment
Exhibit 17	11/1/2019 Huawei Ex Parte (providing an expert report on China's National Intelligence Law)
Exhibit 17-A	Supplemental Expert Report of Dr. Hanhua Zhou
Exhibit 18	11/1/2019 Huawei Ex Parte (providing an expert report on 5G network security)
Exhibit 18-A	Expert Report of Professor Valtteri Niemi
Exhibit 19	11/8/2019 Huawei Ex Parte (rebutting the Clarke Report)
Exhibit 19-A	Rebuttal Report of Jihong Chen to Professor Donald Clarke's Memorandum

Exhibit 20	11/12/2019 Huawei Ex Parte (providing positive international assessments of Huawei's equipment and security)
Exhibit 21	11/14/2019 Huawei Ex Parte (addressing the FCC's alleged authority under the Communications Assistance for Law Enforcement Act)
Exhibit 22	6/1/2018 Competitive Carriers Association ("CCA") Comments
Exhibit 22-A	Declaration of Steven K. Barry
Exhibit 22-B	Declaration of Michael Beehn
Exhibit 22-C	Declaration of Frank Dirico
Exhibit 22-D	Declaration of James Groft
Exhibit 22-E	Declaration of Todd Houseman
Exhibit 22-F	Declaration of Michael D. Kilgore
Exhibit 22-G	Declaration of John C. Nettles
Exhibit 22-H	Declaration of Eric J. Woody